نديم عبده

حروب المستقبل

دور الكمبيوتر والأسلحة غير الفتاكة في النزاعات المستقبلية

استعمال الكمبيوتر في حروب المستقبل

- سيناريوهات الحرب المعلوماتية الشاملة
- الكمبيوتر في حروب المستقبل
- المناورات الأولى لحرب الكمبيوتر
- الأمن الكمبيوتري من الأمن القومي
- القيروسات المعلوماتية
- القيروسات الكمبيوترية في الحروب المستقبلية
- الق... نة المعلوماتية
- ... نة الكمبيوترية على الدوائر الأمنية
- ... لكمبيوتر بين أميركا والصين
- ... المعلوماتي الخاص للأفراد

الأسلحة غير الفتاكة وحروب المستقبل

- أسباب تطوير الأسلحة غير الفتاكة
- أبرز الأسلحة غير الفتاكة
- برامج الأسلحة غير الفتاكة
- سلاح الجو الأميركي والأسلحة غير الفتاكة
- التجارب الأولى للأسلحة غير الفتاكة
- الأسلحة غير الفتاكة في الشرق الأوسط
- الأسلحة غير الفتاكة وأسلحة الدمار الشامل



حروب المستقبل

حروب المستقبل

دور الكمبيوتر والأسلحة غير الفتاكة في النزاعات المستقبلية

استعمال الكمبيوتر في حروب المستقبل

- **سيناريوهات الحرب المعلوماتية الشاملة**
- **الكمبيوتر في حروب المستقبل**
- **المناورات الأولى لحرب الكمبيوتر**
- **الأمن الكمبيوتري من الأمن القومي**
- **الفيروسات المعلوماتية**
- **الفيروسات الكمبيوترية في الحروب المستقبلية**
- **القرصنة المعلوماتية**
- **القرصنة الكمبيوترية على الدوائر الأمنية**
- **حرب الكمبيوتر بين أميركا والصين**
- **الأمن المعلوماتي الخاص للأفراد**

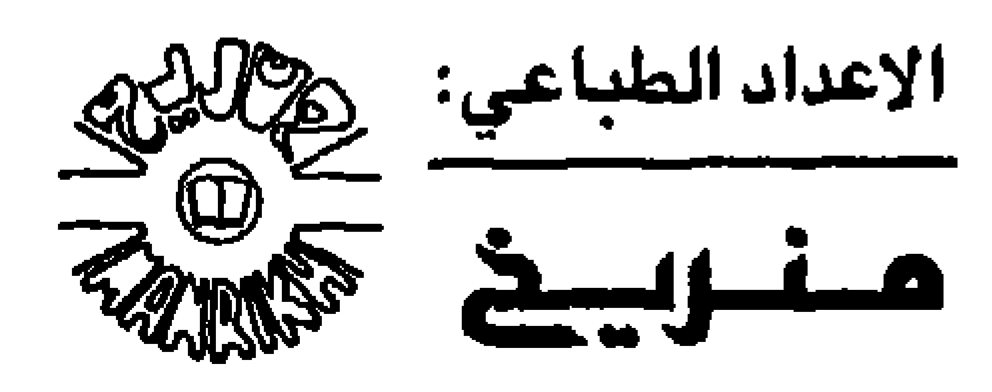
الأسلحة غير الفتاكة وحروب المستقبل

- **أسباب تطوير الأسلحة غير الفتاكة**
- **أبرز الأسلحة غير الفتاكة**
- **برامج الأسلحة غير الفتاكة**
- **سلاح الجو الأميركي والأسلحة غير الفتاكة**
- **التجارب الأولى للأسلحة غير الفتاكة**
- **الأسلحة غير الفتاكة في الشرق الأوسط**
- **الأسلحة غير الفتاكة وأسلحة الدمار الشامل**

صادر عن: نديم عبده
ص.ب 165903 بيروت - لبنان

طبع في سنة 1999

الاعداد الطباعي:



منريخ
للطباعة والنشر والتوزيع
هاتف: 663172

محتويات الكتاب

تمهيد

لقد بدأت صورة الحروب تتبدل بصورة جذرية عما كانت عليه في الماضي مع نهاية الحرب الكونية الثانية، وذلك بفعل ظهور أسلحة الدمار الشامل وتزايد أهمية الاعلام والتقنيات المعلوماتية في تحديد مسار الأحداث.

وينتظر أن تأخذ وتيرة هذه التبدلات بالتسارع مع حلول القرن الحادي والعشرين، وظهور تقنيات جديدة تسمح باتباع أساليب مبتكرة للقيام بالعمليات الحربية تختلف اختلافاً جذرياً عن ما هو معهود.

ويبحث هذا الكتاب في بعض أبرز هذه الأساليب الجديدة، وهو يتألف من قسمين يتناول الأول استعمال التقنيات المعلوماتية في العمليات الحربية، ويتطرق الثاني إلى نوع جديد من الأسلحة يعرف بالأسلحة غير الفتاكة، مع العلم بأن العديد من الخبراء يصنف الأسلحة المعلوماتية في خانة الأسلحة غير الفتاكة. ويأتي هذا الكتاب مكملاً لكتاب« الأنظمة الحديثة للمخابرات».

القسم الأول :

استعمال الكمبيوتر في حروب المستقبل

مقدمة عامة

يلعب الكمبيوتر دوراً أساسياً في مختلف أوجه الحياة في الآونة الراهنة، وذلك منذ أن بدأ يدخل في كل بيت وفي كل مكان للعمل في مختلف بلدان العالم منذ أوائل الثمانينات عندما طرحت أولى الأجهزة الكمبيوترية الشخصية.

ومن الطبيعي إذ ذاك أن يدخل الكمبيوتر في مجال التطبيقات الأمنية والعسكرية من الباب الواسع وذلك إلى درجة بات يتوقع معها العديدون بأن هذا الكمبيوتر بالذات سوف يشكل وحده سلاح المستقبل.

لقد سبق لنا وأن تطرقنا إلى الأمن الكمبيوتري في كتابنا «أمن الكمبيوتر» الصادر عن دار فكر سنة 1991، والذي نقدم فيه شرحاً لماهية الكمبيوتر والجوانب المختلفة من الأمن المعلوماتي، ومن ثم أصدرنا كتاب «حرب الكمبيوتر في فلسطين» سنة 1996 حيث تمّ التركيز على الجوانب المعلوماتية للحرب ضد اليهود داخل وخارج فلسطين المحتلة؛ أما هذا الكتاب الجديد فإنه يسلط الأضواء على دور

الكمبيوتر في الحروب المستقبلية، وذلك لجهة استغلال أعمال القرصنة المعلوماتية وزرع الفيروسات من أجل تخريب البنى التحتية للاعداء مع الاشارة إلى أن كتابنا «الأنظمة الحديثة للمخابرات» يتناول تقنيات التجسس التي تتم بواسطة الكمبيوتر.

ويسعى هذا الكتاب إلى كشف الحقائق وتبديد الأوهام حول دور الكمبيوتر في حروب المستقبل، مع التطرق إلى الأساليب العسكرية الجديدة التي توفرها التقنية المعلوماتية.

الفصل الأول:

سيناريوهات واقعية لحرب معلوماتية شاملة

من الأمور الثابتة في التاريخ أن الحروب ترتدي شكلاً مميزاً في كل عصر، حيث نستعمل فيها أنواع جديدة من الأسلحة؛ وبالعودة إلى القرن العشرين الذي شارف الآن على الانتهاء نرى أن الدبابات والمدرعات البرية كانت الأسلحة الرئيسية خلال الربع الأول منه (وخصوصاً في الحرب الكونية الأولى)، ثم لعبت أسلحة الطيران والبحر الدور الأساسي خلال الحرب الكونية الثانية قبل أن تلعب الأسلحة النووية والصواريخ الاستراتيجية الدور الأساسي اعتباراً من الخمسينات وحتى أوائل التسعينات؛ ومع الانتشار الواسع لتكنولوجيا المعلومات على مختلف المستويات، يبدو أن حروب المستقبل سوف تعتمد على أسلحة «معلوماتية»، والمقصود بأسلحة معلوماتية هو تطوير برامج ومعدات قادرة على تخريب الأنظمة الكمبيوترية للاعداء أو بالتنصت عليها، من قبيل برامج الفيروسات

الكمبيوترية أو أجهزة التشويش أو الأنظمة التي تسمح بخرق أنظمة التشفير البياني... وبالفعل، فلقد أخذت القوى العظمى في عالمنا اليوم تتسابق على تطوير أفضل الأنظمة المعلوماتية العسكرية، وفي طليعتها الولايات المتحدة وروسيا وبلدان الاتحاد الأوروبي.

أما أهداف الأسلحة المعلوماتية، فيمكن اختصارها بأنها خلق حالة من الفوضى الكاملة في صفوف الأعداء عن طريق تخريب الشبكات الكمبيوترية التي تتحكم بأنظمة الأسلحة والمبادلات المالية وأنظمة السير وتوزيع المياه والتيار الكهربائي وغيرها...

وتتميز «الحرب المعلوماتية» بأنها حرب من دون جبهات بمعنى أن «أعمال القتال» تجري في كل موقع وتشمل جميع طبقات المواطنين وليس العسكريين وحدهم، والحرب المعلوماتية لا تؤدي إلى الحاق الأضرار المادية وسقوط الجرحى والقتلى بصورة مباشرة، وإنما «يمكن أن تكون مفاعيلها شبيهة إلى حد بعيد بمفاعيل استعمال أسلحة الدمار الشامل» حسب ما أكد عليه وزير الخارجية الروسي ايغور ايفانوف (Igor Ivanov) في رسالة بعث بها إلى الأمين العام لهيئة الأمم المتحدة (United Nations) في تشرين أول (أكتوبر) 1998.

وتبدو الحكومة الروسية شديدة الاكتراث بالخطر الذي تمثله الحرب المعلوماتية في نهاية التسعينات حيث دعا الروس إلى إبرام اتفاقات دولية من أجل «منع تطوير وانتاج واستعمال الأنواع الخطيرة جداً من الأسلحة المعلوماتية»، مع طلب مناقشة هذه المقترحات في

الدورة العادية التي تعقدها الجمعية العمومية لهيئة الأمم المتحدة لسنة 1999.

ويعود اهتمام روسيا بهذا الموضوع إلى أن حالة الفوضى المستفحلة والفساد المستشري على جميع مستويات الحياة السياسية والاقتصادية في هذا البلد جعلته عاجزاً عن تطوير أنظمته وأسلحته إلى درجة تجعلها متوازية لمستوى التكنولوجيا الغربية (مع التذكير هنا بأن الاتحاد السوفياتي السابق كان يتفوق على الغرب أو يتساوى معه في العديد من المجالات العلمية والتكنولوجية خلال عقدي الخمسينات والستينات من هذا القرن...) علماً بأن هذا التخوف الروسي بات يثير مخاوف الولايات المتحدة نفسها، حيث يؤكد بعض المسؤولين بأن روسيا فشلت فشلاً تاماً في معالجة مشكلة «شائبة العام 2000» وهو الأمر الذي يمكن أن يؤدي إلى تعطيل العديد من الخدمات العامة عند حلول القرن الحادي والعشرين مما قد يحمل حكام روسيا على الاعتقاد بأن هذا التعطيل حصل نتيجة «لاعتداء أميركي» على روسيا، فيعمدون إلى الرد على هذا الاعتداء المعلوماتي المزعوم عن طريق شن حرب نووية...

والواقع أن الحكام الأميركيين أنفسهم يتخوفون من أن تتعرض الولايات المتحدة لهجوم معلوماتي شامل تكون نتائجه مشابهة لنتائج الهجوم الياباني على القاعدة البحرية الأميركية في بيرل هاربر (Pearl Harbor) سنة 1941. وهو الهجوم الذي أدى إلى دخول الولايات المتحدة

الحرب الكونية الثانية إلى جانب بريطانيا والاتحاد السوفياتي في مواجهة اليابان والمانيا.. ويتم حالياً في الولايات المتحدة دراسة أساليب الحرب المعلوماتية وتطوير أنظمة هذه الحرب ويكتنف هذه الأبحاث غطاءً كثيفاً من السرية المطبقة يشبهه بعض المراقبين بغطاء السرية الذي كان يكتنف الابحاث النووية الأميركية أوائل الاربعينات.

وتقول بعض المصادر بأن هذه الأبحاث الأميركية أسفرت عن تطوير فيروسات من نوع «الفيروسات الديدانية» (worm viruses) (وهي الفيروسات التي تنقل بواسطة الشبكات الكمبيوترية الموضعية وتتفشى في ذاكرة الجهاز الكمبيوتري عن طريق «التناسخ» مع الانتشار في جميع الأجهزة الكمبيوترية المرتبطة بالشبكة)، وقامت بزرع هذه الفيروسات في عدد من الشبكات خارج أميركا من أجل إحداث حالة من الفوضى في صفوف «اعداء أميركا».

وتبرر وزارة الدفاع الأميركية القيام بتطوير هذه الأسلحة بأن لكل من روسيا والصين والعراق وليبيا برامج أبحاث مماثلة...

وكان الرئيس الأميركي بيل كلينتون أعلن في أيار (مايو) 1998 عن اتخاذ الحكومة الأميركية اجراءات «دفاعية» للحؤول دون حصول معركة «بيرل هاربر رقمية» إلا أن مجهود أميركا لا يقتصر أبداً على تطوير أنظمة دفاعية، حيث أكد مدير وكالة المخابرات المركزية الأميركية «سي آي أي» (CIA) بأن أميركا بدأت تستعمل أسلحتها المعلومأتية سنة 1997 في «حربها ضد الارهاب والمخدرات»،

واستعملت تقنيات القرصنة المعلوماتية لعرقلة حركة التحويلات المالية الدولية الخاصة برجال أعمال عرب «يدعمون ارهابيين» (على حد زعم الأميركان طبعاً).

كما يؤكد بعض الروس بأن وكالة سي آي أي قامت بتخريب بعض الأنظمة الكمبيوترية التي تم تصديرها من أميركا إلى بلدان الاتحاد السوفياتي السابق، وذلك عن طريق زرع هذه الأنظمة «بشوائب» تسمح لعملاء الوكالة بقرصنتها من على بعد آلاف الأميال...

ولقد وضعت حكومة الرئيس كلينتون خطة مدتها خمس سنوات لجعل أميركا محمية من المخاطر المعلوماتية، وهي المخاطر التي يمكن أن تؤدي إلى نشوب حرب حقيقية.

ولقد وصف تقرير صادر عن وزارة الدفاع الأميركية سيناريو اندلاع حرب معلوماتية على الوجه التالي: ينقطع التيار الكهربائي في مدينة رئيسية على نحو لا يمكن تفسيره، وتصبح الشبكات الهاتفية في جميع أنحاء البلاد مشلولة، كما يؤدي تخريب الأنظمة المعلوماتية إلى حصول حوادث اصطدام بين القطارات وتدب الفوضى في شبكات مراقبة حركة الطيران، كذلك في شبكات خطوط الأنابيب النفطية والغازية، مما يؤدي إلى انفجار محطات لتكرير النفط...

كذلك فإن استشراء الفيروسات المعروفة بالقنابل المنطقية (logic bombs)، (وهي الفيروسات التي تنطلق عند تشغيل مفتاح أو رقم أو كلمة معينة على الكمبيوتر، أو عند حلول تاريخ محدد) يؤدي إلى

تعطل النظام المالي العالمي مع خربطة التحويلات المالية وحركة مبادلات أسواق تبادلات الأسهم والسندات، فضلاً عن تعطيل أجهزة الصرف الآلي أو أنظمة البطاقات الائتمانية..بالاضافة إلى تخريب الأسلحة المعتمدة على النظم المعلوماتية.. ويؤدي كل هذا إلى شن الدولة المستهدَفة (بفتح الدال) بهذا الهجوم المعلوماتي هجوماً عسكرياً ضد الدولة التي تعتقد بأنها المعتدية (بكسر الدال) عليها..

ولم يعد موعد المباشرة في حرب معلوماتية حقيقية بعيداً جداً، وفق تقديرات الخبراء، وقد أجرى العسكريون الأميركيون «مناورات معلوماتية» من أجل دراسة الامكانات العملية لاستعمال النظم الكمبيوترية من أجل الحؤول دون نشوب حرب نووية بين الهند والباكستان في سنة 1997 عن طريق تخريب النظم الكمبيوترية في البلدين، ولم تعرف نتيجة هذه المناورات إلا أن الأمر الأكيد هو أن الحروب المستقبلية سوف تكون معلوماتية قبل أن تكون عسكرية...

الفصل الثاني:

دور الكمبيوتر في حروب المستقبل كما يراه الأميركيون

يعتبر القضاء على البنى التحتية في دولة ما من الشروط الأساسية التي تؤمن النصر العسكري لدولة معادية لها في حرب تجري بينهما، والبنى التحتية المقصودة هي خطوط الاتصالات والمصانع الأساسية والمزارع الرئيسية وشبكات المواصلات.

ولقد تحولت الأنظمة والشبكات الكمبيوترية منذ أوائل الثمانينات إلى جزء أساسي من البنى التحتية، حيث تعتمد هذه الأنظمة للقيام بجميع أنواع الأعمال من صناعية ومالية وثقافية، فضلاً عن اعتماد الشبكات الكمبيوترية لتأمين الاتصالات ولتبادل المعلومات.

وكان من الطبيعي اذ ذاك أن يدرس الخبراء العسكريون بعناية فائقة أفضل السبل الكفيلة بالقضاء على الأنظمة الكمبيوترية المعادية! وقد وصل الأمر إلى درجة ثم معها تشكيل فرق متخصصة تابعة للقيادات العسكرية في بعض البلدان المتقدمة، وهي مولجة فقط أمر القيام بالعمليات العسكرية الكمبيوترية، وذلك من دون أن يتطلب

القيام بهذه العمليات استعمال أي نوع من أنواع الاسلحة النارية، وإنما فقط السعي لتخريب الأنظمة الكمبيوترية المعادية عن طريق زرعها بالفيروسات المعلوماتية، كما أن هذه الفرق مسؤولة عن حماية الأنظمة الكمبيوترية في بلدها، وهي مولجة أمر تحديد واختيار الأجهزة والبرامج المناسبة لتستعملها القوات الأسلحة ودوائر المخابرات.

وتقدم في ما يلي مقتطفات من مقالة أعدها أحد المسؤولين الأميركيين حول حرب المعلوماتية، وتلقي الأضواء حول نظرة القيادة العسكرية الأميركية لدور المعلوماتية في حروب المستقبل، مع الاشارة إلى أن الآراء الواردة في هذه المقتطفات تعبر عن وجهة النظر الأميركان وليس عن وجهة نظرنا...

«مع دخول الانسانية عصر ما يعرف بالمجتمع ما بعد الصناعي (Post- industrial society)، وهو العصر الذي يعرف بعصر مجتمع المعلومات (information society) (إشارة هنا إلى أن علماء الاجتماع يقسمون الفترات التاريخية حسب النشاط الاقتصادي الرئيسي فيها، حيث أن النشاط الصناعي كان الغالب طيلة القرن التاسع عشر وحتى منتصف القرن العشرين، ويعتبرون أن العصر الجديد هو عصر المعلوماتية)، فلقد بات المحترفون العسكريون شاعرين بأهمية المعدات الحربية المعتمدة على تكنولوجيا المعلومات. غير أن هذا التطور لا يزال قائماً على مفاهيم قديمة تبقى صالحة إلى جانب المفاهيم الجديدة.

ولقد كان أمر الحصول على معلومات حول قوة ومواقع وامكانات الاعداء مع الحؤول دون حصول هؤلاء الاعداء على المعلومات عاملاً أساسياً في الحرب على مدار التاريخ.

وتأخذ المعلومات أهمية متزايدة باطراد كلما تقدمنا في عصر تكنولوجيا المعلومات.

مثال على ذلك أنه يبدو من المؤكد أن القوات المسلحة الأميركية سوف تستمر متدخلة في أماكن بعيدة عن الولايات المتحدة، وإنما مع كمية أقل من موارد الدعم اللوجستي. وعلينا (أي على الأميركيين) أن نتعامل ليس فقط مع العوامل العسكرية التقليدية - القدرات العسكرية اللوجستية - وإنما أيضاً مع احتمال حصول أعدائنا على تكنولوجيا معلوماتية أكثر تطوراً.

ولقد جعل طغيان وسائل الاعلام على الحياة العامة في جميع المجالات من الصعب، حتى لا نقول من المستحيل، القيام بعمليات عسكرية مفاجئة، أو رسم استراتيجيات سرية. وسوف تتيح امكانات عصر المعلومات للاعداء امكانية الحصول على معلومات قيمة حول امكانات الولايات المتحدة.

وإذا أضفنا إلى ذلك تزايد قوة أعداء أميركا فإننا نجد أن قدرة الولايات المتحدة القيام بعمليات في الخارج باتت معرضة للخطر.

إن أعداءنا المحتملين قد يضعون حلفاءنا الاقليميين في الخطر لردعنا عن التدخل. وقد يعمدون إلى التسبب لحلفائنا بخسائر كبيرة

قبل أو خلال تدخلنا الميداني. وهذه من الدروس المستقاة من حرب الخليج.

إن تعزيز تفوقنا في مجال أنظمة المعلومات والقيادة يمكن أن يتم عن طريق جعل أنظمة المعلومات والقيادة والمراقبة الخاصة باعدائنا معطلة جزئياً أو كلياً، وكذلك الأمر بالنسبة إلى الحفاظ أو إلى تقوية انظمتنا الخاصة للقيادة والمراقبة والاتصالات والكمبيوتر والمعلومات.

وأمر تأمين امكانية تنظيم عمل عدة قوات متحالفة في عملية عسكرية مشتركة هو بنفس أهمية الحؤول دون تمكن العدو من تنسيق عمل قواته. وسوف تتيح تكنولوجيا المعلومات أمام القوات الأميركية وضع خطط مفصلة ومكتملة للمعارك بصورة سريعة مع تعديلها عند اللزوم، وذلك بالاعتماد على الذكاء الاصطناعي وأنظمة التشبيه.

بالاضافة إلى ذلك فسيكون بإمكان القائد الأعلى للقوات المتدخلة نقل خططه كما هي مرسومة على الخرائط حتى أدنى المستويات. وعند تحقيق انجاز عسكري أو عند بروز فرص عسكرية غير متوقعة، فإن القادة الأقل درجة سوف يستطيعون الاستفادة الكاملة من الوضع المستجد بسرعة، بالنظر إلى حصولهم على صورة مكتملة للوضع العسكري ككل.

لقد بات بإمكان المجموعات والافراد الحصول على معلومات

تتعدى جميع حدود البلدان بسهولة اليوم مع المعدات المتوافرة حالياً. إن وضع حاجز واضح بين المعلومات المتوفرة أمام الجميع والمعلومات السرية من الأمور الضرورية جداً للحفاظ على تفوقنا.

وثانياً فإن الحفاظ على سلامة أنظمة المعلومات لدينا، من الأمور الأساسية. وسوف تحصل المواجهات المستقبلية ضد قوات معادية قد تكون متفوقة في مجال القوة العسكرية التقليدية. وجمع المعلومات ثم توزيعها على القوات الصديقة من الأمور الأساسية. مع وجوب وضع شبكة متينة من أنظمة القيادة والمراقبة. والاتصالات والكمبيوتر والمعلومات قبل اندلاع الحرب بمدة طويلة. وعلى المحاربين حماية معلوماتهم إلى أقصى درجة ممكنة.

وأخيراً فإن قدرتنا على ازالة التسرب وإلى تعطيل أو تدمير أنظمة معلومات العدو سوف يكون من شأنها تعزيز تفوقنا على أعدائنا، ويتم ذلك باستخدام الأسلحة الفتاكة أو الالكترونية. والهدف الأساسي أن تمنع العدو من الولوج إلى المعلومات الخاصة به نفسه.

إن التفوق التجاري الأميركي في مجال تكنولوجيا المعلومات جعل قواتنا الأسلحة قادرة على القيام بحروب تعتمد على المعلومات. وحتى الآن فإن هذه الامكانية زادت فعالية الأشكال التقليدية من الأساليب الحربية إلا أن شكلاً ثورياً فعلاً من المعدات الحربية سوف يظهر مع اختمار عصر المعلومات.

إن معدات الحرب المعلوماتية سوف تسير في محيط يختلف عن

ميادين الحرب التقليدية، مع اعداء مشتتين في الآفاق المعلوماتية. ومع ولوج أي من الأعداء المحتملين إلى أنظمة المعلومات المتعددة. فإن الحرب سوف تسير بصورة ظاهرية وبسرعة الضوء عبر كل المسافات.

إن السيطرة على مجالات عصر المعلومات قد تخفف الحاجة إلى استعمال الأسلحة النارية التقليدية. (المقصود بمجالات عصر المعلومات cyberspace هو السيطرة على مصادر المعلومات الموزعة على أنظمة الاتصالات والعرض المختلفة). أن أساليب الحرب التقليدية تعكس اراء المنظر العسكري الالماني كارل فون كلوتيز (Karl Von Clauwitz) بأن القوات العسكرية لامة ما يجب أن تتفوق على قوات أعدائها لفرض ارادتها على العدو وبلوغ أهداف أساسية. إلا أن هذا الرأي قد لا يكون مناسباً اليوم.

إن مفهوم الحرب الذي نادى به العالم الاستراتيجي الصيني القديم صات تسوهو هو الذي حدد مفهوم حرب المعلومات، وهذا المفهوم يقول بأن النجاح يكمن في تفادي الاشتباكات وفرض تحقيق الهدف عن طريق مناورات ذكية واستغلال مواقع ضعف الخصم. إن الدخول إلى أنظمة معلومات العدو في مجالات عصر المعلومات بدل من الانتصار على ساحة المعركة سوف يقنع العدو بأن الاشتباكات التقليدية أو غير التقليدية ستكون تافهة.

إن تحقيق الردع التقليدي سوف يكون من الأمور التي تزيد

صعوبة تحقيقها. وفي حين أن الولايات المتحدة ستكون قادرة إجمالاً على ارسال قوات متفوقة لاحتواء توتر اقليمي. فمن الصعب التكهن بنيات رؤسائنا المنتخبين بصورة ديموقراطية، وخصوصاً من الصعب أن تتكهن أنظمة طغيانية (ديكتاتورية) غير معتادة على نمط تسيير السياسة في البلدان الغربية ماهية هذه النيات.

إننا سنكون قادرين على اثبات أهدافنا الواضحة وقدرتنا على استخدام قوة حاسمة عن طريق استغلال ميدان معركة المعلومات بسياسة خارجية قوية. وفي حال فشلت سياسة الردع هذه فإن تقنيات وامكانات حرب المعلومات لن تتيح لنا القيام بردود فعل أسرع مما لدى عدونا وحسب وإنما السيطرة على أنظمة اتخاذ ونقل القرارات الخاصة به وجعل عملياته العسكرية (أي العمليات التي يقوم بها العدو) تسير وفق مسالك غير فعالة ويمكن توقعها.

لقد حان الوقت لأن تنفتح اذهاننا وأن نستغل الفرص الثورية التي توفرها حرب المعلومات في حروب المستقبل».

ويتضح من جراء هذه المقالة بأن الولايات المتحدة تعتبر أن التفوق في حرب المعلومات هو شرط أساسي لضمان التفوق في الحرب ككل..

اشارة أخيراً إلى أن معظم البرامج الكمبيوترية التي تستعمل لتسيير مرافق البنى التحتية تعتمد على أنظمة تشغيلية معروفة جيداً لدى جميع مستعملي الكمبيوتر، وبالتالي فإن التغلغل إليها وزرعها

بالفيروسات ليس من الأمور البالغة الصعوبة بالنسبة إلى خبراء معلوماتيين من الناحية المبدئية.

ملحق

المناورات الأولى لحرب الكمبيوتر
وتشكيل أولى الفرق المعلوماتية العسكرية

كشفت وزارة الدفاع الأميركية عن اجراء مناورة عسكرية مع القيام بأعمال هجومية بواسطة الكمبيوتر في 1997. فقد تولى سلاح الجو الأميركي إجراء هذه المناورات، وكان الهدف منها دراسة السبل التي تستطيع فيها الطائرات العسكرية الاميركية حماية الأنظمة الكمبيوترية، وتمت العمليات في ولاية ألاسكا شمالي الولايات المتحدة، ودامت أسبوعين.

أحيطت هذه المناورات بالسرية المطلقة، إلا أنه علم بأن العمليات الهجومية الكمبيوترية استهدفت أنظمة المراقبة والأمن في شبكات الاتصالات اللاسلكية والهاتفية، فضلاً عن قرصنة البيانات المخزنة في أنظمة كمبيوترية غير محمية.

ويعتقد بأن كلاً من وكالة الأمن القومي (National Security Agency) و«وكالة أنظمة المعلومات الدفاعية (Defence Information Systems Agency) ووكالة المخابرات الجوية (Air Intelligence Agency) قد شاركت في هذه المناورات وفي التدريبات التي خضع لها العسكريون الذين ساهموا فيها. وقدمت هذه الوكالات توصيات حول

كيفية تحسين الأجهزة والبرامج لتحسين مستوى العمليات والدفاعات الكمبيوترية.

وأعقب ذلك بذل الادارة الأميركية جهوداً حثيثة من أجل تشكيل أولى الفرق العسكرية المتخصصة في أعمال الحرب الكمبيوترية، مع حصول نقاشات حامية حول من يجب أن يتولى قيادة تلك الفرقة من بين أسلحة الجو والفضاء والبر والبحر...

وكانت بعض الجهات قد اقترحت أن تتولى قيادة الفضاء في الجيش الأميركي ادارة العلميات المعلوماتية، وذلك على أساس أن معظم الاتصالات الكمبيوترية تتم بواسطة الأقمار الصناعية. في حين يطرح البعض الآخر انشاء قيادة جديدة متخصصة.

بالمقابل أكد قادة سلاح الجو بأن سلاح الطيران يمكن أن يلعب دوراً رئيسياً في عمليات هجومية كمبيوترية، ومن الأمثلة على ذلك أنه تم اختبار طائرات دون طيار محملة بأنظمة الكترونية قادرة على التقاط الموجات اللاسلكية المتنقلة بين الابراج المخصصة لبث واستقبال الميكروموجات، وبعدها تستطيع هذه الطائرات استبدال هذه الموجات ببيانات خاطئة أو معدلة يعاد ارسالها إلى الأجهزة الكمبيوترية المستقبلة للرسائل، وبذلك يتلقى القادة العسكريون أوامر مغلوطة حول كيفية قيامهم بالعمليات العسكرية.

وانتهت هذه النقاشات على نحو موقت بأن دخلت الفرقة العسكرية الأميركية المتخصصة في القيام بأعمال الحرب المعلوماتية

الخدمة «الميدانية» الفعلية في الثلاثين من كانون أول (ديسمبر) من العام 1998، وثم تعيين الميجور جنرال جون كامبيل.(John Campbell) قائداً لها، وهو ضابط كان يعمل سابقاً في صفوف سلاح الجو الأمركي (Us Air Forcè).

وتعرف هذه الفرقة بـ «القوة العسكرية للدفاع عن شبكات الكمبيوتر». (Joint Task Forve on Computer Network Defence)، وهي تعمل بالاشتراك مع القيادات المشتركة لاسلحة البر (Army) والبحرية (Navy) والجو (Air Force) ومشاة البحرية (Marines) ودوائر أخرى تابعة لوزارة الدفاع الأميركية على التصدي لعمليات القراصنة المعلوماتيين الذين يستهدفون الشبكات الكمبيوترية الأميركية.

وستساهم الفرقة كذلك في وضع استراتيجية على المدى الطويل للدفاع المعلوماتي.

وما تزال الفرقة متواضعة في 1999، مع ميزانية لا تتجاوُز قيمتها 5,2 مليون دولار. وهي تعمل على تحديد مفاهيم العمليات والتكتيكات والتقنيات والاجراءات المطلوبة لمجابهة التهديدات المعلوماتية، وذلك بالتعاون مع القادة الاقليميين للمناطق العسكرية الاميركية.

وتتركز أعمال الفرقة على ثلاث مهمات:

- تدريب وتعليم العسكريين ليتعرفوا على ماهية الحرب المعلوماتية وكيفية التصدي لها.

- تحديد الاجهزة والمعدات المعلوماتية التي تضمن حد أدنى من

- اختيار البرامج المعلوماتية المناسبة لتزويد الاجهزة بها.

كما أن هذه الفرقة مسؤولة عن تزويد الفرق العسكرية بالدعم التقني مع تقديم المشورة عندما تتعرض إلى هجمات معلوماتية.

وللفرقة صلاحية الاضطلاع بقيادة عمليات مشتركة تقوم بها عدة أسلحة أميركية وسوف تُستبدل هذه الفرقة المشتركة بقوة عسكرية ثابتة تتخصص للحروب المعلوماتية في السنوات القليلة المقبلة بعد أن تكون ملامح الحرب المعلوماتية قد توضحت وتحددت بصورة نهائية.

الفصل الثالث:

الأمن الكمبيوتري من الأمن القومي

تعتمد الشركات العالمية على شبكات المعلوماتية لتبادل المعلومات وتحويل الأموال، وذلك إلى الدرجة التي أصبحت فيها هذه الشبكات جزءاً لا يتجزأ من عملها. وكان من الطبيعي إذ ذاك أن ترتدي أعمال التعرض والاعتداء على مصالح الشركات اشكالاً «معلوماتية». وبالفعل بدأت تحصل حوادث عدة من هذا النوع في السنوات الأخيرة، وينتظر أن تتعزز هذه الظاهرة في القرن الحادي والعشرين، بحيث تصبح الجرائم «الرائجة» هي القرصنة المعلوماتية وزرع الفيروسات الكمبيوترية في أنظمة الشركات المستهدفة، وليس القيام بهجمات مسلحة على المباني والمصانع بهدف الاستيلاء على الأموال والسلع.

يمكن تلخيص المخاطر الناجمة عن الاعتداءات المعلوماتية بالآتي:

- تعطيل الأنظمة الكمبيوترية بصورة كاملة مع ما يسفر عن ذلك من نتائج سلبية على صعيد خسارة الصفقات وتدهور السمعة في الأسواق المالية والتجارية.

- تعطيل جـزئي للأنظمـة المعلومـاتيـة مع تكبـد الشـركـة الضـحـيـة تكاليف باهظة لاصلاح الأعطال.

تؤكد عدة مصـادر مطلعة بأن جماعات ثورية أو ارهابية (حسب التـصنيف الخـاص بكل طرف....) مـثل منظمـة الانفـصـاليين الباسك «الايتـا» (ETA) والجـيش الجـمـهـوري الايرلندي (IRA) أو جـمـاعـة الثـوريين المكسـيكيين (الزاباتيون) قد تكون بدأت بالفعل القيام بهذه الأعمال وذلك على الوجه الآتي:

- تقـوم المنظمـة الثـورية بزرع فـيروس في الشـبكة الكمـبـيـوترية للشـركة المسـتـهدَفة (بفتـح الدال)، ويكون بإمكان هذا الفيـروس تعطيل النظام بأسـره. وتطالب المنظمـة الشـركـة بدفع الأمـوال مـقـابل نزع الفيروس، وإلا عمدت إلى تعطيل الشبكة بكاملها.

مـعروف أن العـديد من الجـيـوش يدرس أيضـاً الامكانات العـمليـة لاسـتـغلال هذا النوع الجـديد من الأسـاليب العـسكرية في المسـتقـبل، وذلك إمـا بصـورة مـباشـرة أو بواسطة جماعـات ارهابيـة وهمـيـة تمثل التغطية أو القناع الرسمي للعملية العسكرية الكمبيوترية.

أما أبـرز الوسـائل التي يمكن للاعداء من خلالها التسـرب إلى النظم المعلوماتية، فهي التالية:

- التعـرف إلى كلمات السـر للولوج إلى النظم الكمـبيـوترية بواسطة موظفين سـابقين للشـركة المسـتـهدفة(بفتح الدال)، وخـاصـة إذا كانت ادارة الشـركة قد أهملت وجـوب تبديل كلمـات المرور بصـورة دورية،

وهذا ما يفترض فعله للحفاظ على مستوى جيد للأمن الكمبيوتري.

- التعرف إلى أسرار الشبكة الكمبيوترية المستهدفة بواسطة متعاقدين خارجيين مع صاحب الشبكة يعملون في مجالات البرمجة والصيانة.

- إمطار الأنظمة الكمبيوترية التي يتم فيها تخزين قيود الشركة باشعاعات لاسلكية ذات نسبة تردد مرتفعة ويكون من نتيجة هذا العمل محو البيانات التي تكون قد تعرضت لهذا «الوابل» الكهرومغناطيسي.

يشار إلى أن هذا الخطر لا يزال يبدو بعيداً في الوقت الحاضر بالنظر إلى أن عملية «الامطار» هذه تتطلب قدراً كبيراً جداً من الطاقة الكهربائية ويصعب نقل آلات توليد هذه الطاقة على مقربة من المكاتب التي تتواجد فيها الأنظمة الكمبيوترية المستهدفة (بفتح الدال)، إلا أن التكنولوجيا تتقدم يوماً بعد يوم ومن غير المستبعد أن تصنع قريباً آلات صغيرة تولد اشعاعات كهرومغناطيسية قوية سهلة النقل.

أما الاجراءات التي يجب على الشركات أن تتخذها لمواجهة هذا النوع من المخاطر، فيتمثل أبرزها بوجوب وضع خطة وقائية لتخفيف وطأة المخاطر.

يمكن تلخيص أبرز ما يجب أن تتضمنه هذه الخطة بالآتي:

- وضع القيود المعلوماتية في اقراص احتياطية تُحفظ في أماكن آمنة، بحيث لا تسفر عملية «الاعتداء» على محتويات الذاكرة

الكمبيوترية عن خسارة جميع هذه القيود بصورة نهائية.

- تشفير البيانات الكمبيوترية الخاصة بالشركة.

- اعتماد سياسة منظمة لتُبدل كلمات المرور بصورة دورية وتحديد الأشخاص المولجين معرفة هذه الكلمات بصورة دقيقة.

- دراسة أنواع الاعتداءات الكمبيوترية المحتملة ووضع «خطط طوارىء» لمواجهة كل نوع من الاعتداءات.

- في حال التعرض الفعلي لعملية ابتزاز، يجب اطالة التفاوض مع الطرف الذي يمارس الابتزاز بالقدر الممكن مع محاولة استغلال مدة المفاوضات للتعرف قدر المستطاع إلى هوية المبتزين وإلى ما إذا كانت تهديداتهم جدية فعلاً أم لا.

هذا، ويجب أن لا يغيب عن البال بأن الشركات الخاصة ليست الوحيدة المستهدفة بهذه المخاطر، وإنما أيضاً الدوائر الحكومية ومصالح القطاع العام، وبالتالي فإن الحفاظ على الامن الكمبيوتري بات من العوامل الرئيسية للحفاظ على الأمن القومي للدول.

ملحق

أنظمة تصفيح أجهزة الكمبيوتر الشخصي

من المعروف أن أجهزة الكمبيوتر هي مصدر قوي لانبعاث الاشعاعات الكهرومغناطيسية وهو الأمر الذي يجعلها عرضة لأعمال المراقبة بمجرد التقاط وتحليل هذه الاشعاعات.

ولقد عمدت بعض الحكومات الغربية إلى تطوير تقنية تحول دون انبعاث الاشعاعات الكهرومغناطيسية من الكمبيوتر إلى مدى يمكن التقاطها، وتم تحديد معايير دقيقة لدرجات التصفيح في الولايات المتحدة تعرف بمعايير تمبست (TEMPEST)، وهذه المعايير سرية ولا تطلع عليها سوى الشركات التي تعتمدها وزارات الدفاع في الدول الغربية.

نذكر أن انتشار المراقيب والشاشات الكمبيوترية التي تصنع وفق تقنية وحدة العرض بالبلور السائل (Liquid Crystal Display) تحتاج إلى طاقة كهربائية بنسبة منخفضة للفولتية، وهو ما يؤدي إلى انخفاض مقدار الاشعاعات الكهرومغناطيسية المنبعثة عنها.

بيد أن المراقيب ليست المصدر الوحيد للاشعاعات، حيث تبين أن الاسلاك المتتالية المعروفة بمعايير أر اس 232 (RS- 232) تبث أيضاً اشارات يمكن التقاطها بسهولة نسبية، وكذلك الأمر مع أسلاك ايترنت (Ethernet). والتقاط الموجات المنبعثة من الأسلاك يتطلب

وجود أجهزة الالتقاط على مقربة من مصدر الاشعاع، الجدير ذكره أن هذه الأسلاك تنقل كلمات المرور ومفاتيح التشفير بطريقة «مكشوفة» على عكس المراقيب الكمبيوترية، وهو ما يؤدي إلى إمكانية التعرف إلى هذه الشيفرات بواسطة شريحة للتسجيل والتوصيل توضع على مقربة من السلك...

يبقى أن هناك أيضاً تقنيات عسكرية سرية لتصفيح الأسلاك...

وأخيراً وليس آخراً، لا بد من الاشارة إلى أن انتيشار أنظمة التوصل دون أسلاك وبواسطة الاشعة ما دون الحمراء من شأنه تسهيل مهمة من يرغبون في التجسس على نشاط الأجهزة الكمبيوترية، إذ يسهل التقاط الموجات ما دون الحمراء عند إجراء عملية توصيل لهذه الأشعة، مثلاً بين كمبيوتر وجهاز طابعة...

الفصل الرابع:

بعض أنواع الفيروسات المعلوماتية

يستحيل ذكر جميع أنواع الفيروسات، بل ويستخيل تصنيفها بصورة دقيقة بالنظرة إلى تكاثرها وظهور أنواع جديدة منها في كل يوم، ولقد كان لانتشار ولتوسع شبكة الانترنت أثره الكبير على تفشي آثار الفيروسات وعلى تحولها إلى آفة حقيقية وذلك بالنظر إلى أنه بات بإمكان أي مشترك على هذه الشبكة اطلاق فيروس جديد ونشره على نطاق عالمي شامل...

ونقدم هنا أمثلة على بعض الأنواع النموذجية للفيروسات الكمبيوترية مع التشديد على أن هذه القائمة غير كاملة، وأن على كل من يريد معرفة المستجدات على هذا الصعيد متابعة الأخبار المتعلقة بهذا الموضوع في وسائل الاعلام أول بأول، وخاصة على مواقع الانترنت المتخصصة، وأو في الصحافة المعلوماتية:

- فيروس فورم (Form): هذا الفيروس يصيب قطاع التأهيل على الأقراص الصلبة واللينة، ويلغي مفعول مفاتيح التشغيل في الرابع

والعشرين من كل شهر.

- فيروس ستوند (Stoned): وهو يصيب أيضاً قطاع التأهيل في القرص الكمبيوتري.

- فيروس باريتي بي (Parity B): فيروس يصيب قطاعات القرص الكمبيوتري واجزاءها، وهو ذو تسهيلات «خفية» بمعنى انه قادر على الاختفاء من الذاكرة.

- فيروس ريبر (Ripper): هذا الفيروس يصيب قطاع التأهيل والاجزاء الأخرى في القرص. ومن مميزاته أنه يبدل شيفرته المصدرية باستمرار. ويمكن زرعه في الأجزاء المختلفة من القرص الأمر الذي يجعل عملية القضاء عليه أمراً صعباً للغاية.

- فيروس ايكزباغ (Exebug): هذا الفيروس يصيب ذاكرة سي أم أو أس (CMOS)ويجعل من الصعب استكمال عملية التأهيل، وعملية استئصاله تتطلب اختصاصيين.

- فيروس «امباير مونكي» (Empire Monkey): هذا الفيروس هو ذو خصائص خفية، ومن شأنه تعطيل عمل القرص الصلب. ويسهل كشف الفيروس لكن يصعب القضاء عليه بسهولة.

- فيروس تيكيلا (Tequila): هذا الفيروس هو ذو ميزات خفية أيضاً وهو ينعكس على الشاشة الكمبيوترية، وهو مؤذ جداً إلا أنه يسهل كشفه والقضاء عليه.

- فيروس كاسكاد (Cascade): هذا الفيروس معروف جداً، وهو

يصيب الأحرف المعروضة على الشاشة.

ومن الأمثلة على الهجمات الفيروسية الكمبيوترية أن 1400 مشتركاً على شبكة الانترنت في أوستراليا تعرضوا في 1998 لهجوم من برنامج فيروسي متخصص في أعمال التجسس. ويعرف ببرنامج «باك أوريفيس» (Back Orifice) (أي الثغرة الخلفية)، ومن شأن هذا البرنامج خلق نظام يتيح لمن يشغله التجسس على أجهزة الكمبيوتر المعتمدة على نظامي وندوز 95 (Windows 95) أو وندوز 98 (Windows 98).

ويمكن ايصال البرنامج إلى الأجهزة المستهدفة عن طريق توصيله ببرامج عادية مطروحة على شبكة الانترنت مثل برامج الألعاب أو البريد الالكتروني وغيرها، بحيث أن من يريد الحصول على تلك البرامج «العادية» وانزالها (downloading) إلى جهازه الخاص يقوم في الوقت نفسه بانزال برنامج التجسس، من دون وعي منه للأمر. وعندما يكون برنامج باك أوريفيس قد أنزل داخل الكمبيوتر، (وتحديداً داخل القرص الصلب في الكمبيوتر) يصبح بإمكان قرصان كمبيوتري الاتصال به (أي بالبرنامج) بواسطة خطوط الانترنت والاطلاع بواسطته على البيانات السرية المخزنة في القرص من قبيل كلمات المرور وأرقام التعريف وغيرها.

وتبين بأن هذا البرنامج التجسسي قد تسرب إلى نحو 1400 كمبيوتر أوسترالي مرتبط بشبكة الانترنت، ومن بينها أجهزة خاصة

بجامعات ومدارس وشركات متخصصة في تأمين الخدمات على شبكة الوب (Web).

هذا، ولقد ذُكر بأن البرنامج كان قد تم تطويره في شهر آب (أغسطس) 1998 من أجل «لفت الانتباه إلى الثغرات الامنية في الأنظمة التشغيلية من شركة مايكروسوفت (Microsoft) التي تنتج أنظمة وندوز.

من ناحية مقابلة، أفادت الاخبار بأن فئة جديدة من الفيروسات الكمبيوترية الخاصة بشبكة الانترنت بدأت تتفشى، وهي فيروسات يتم ادخالها ضمن الصفحات الالكترونية الخاصة بمواقع وب، أو صفحات البريد الالكتروني، ومن غير أن يمكن اكتشافها . وما يزال انتشار هذا النوع من الفيروسات محدوداً في أول 1999 إلا أنه يشكل خطراً بالغاً على مستعملي الكمبيوتر في المستقبل، وذلك بالنظر إلى أن مستعملي الكمبيوتر يمكن أن يتسببوا بتحريك الفيروس بمجرد الولوج إلى موقع على الانترنت يكون مصاباً بها، أو بمجرد تلقي صفحة الالكترونية تتضمن الفيروس من ضمن البريد الالكتروني.

وبإمكان هذه الفيروسات التسبب في اتلاف الملفات الكمبيوترية المصابة بالفيروسات.

وكذلك الأمر مع البرامج الكمبيوترية المحررة بلغة فيجوال بايزيك سكريبت (Visual Basic Script)، وهي اللغة التي يستعملها معظم مطوري مواقع الوب (Web) عند اعداد الصفحات الالكترونية الخاصة

بها. حيث يمكن تطوير فيروسات من هذه الفئة لقرصنة البيانات أو تعطيل أجهزة الكمبيوتر أو خلق ثغرات أمنية على مواقع الانترنت، خصوصاً وأن هذه اللغة منتشرة بكثرة، وهناك عدة لغات كمبيوترية مشابهة معرضة أيضاً للاصابة بهذه الفئة من الفيروسات.

ولم تُطور حتى الآن علاجات كمبيوترية ناجعة وحاسمة لمواجهة هذا الخطر من نوع جديد، وما يمكن فعله ازاء هذه الفيروسات الشبكية هو أخذ جانب الحيطة والحذر عند تلقي بريد الكتروني من مصدر مجهول، مع نسخ البرامج الكمبيوترية الحيوية، ووضعها في مراكز محمية.

الفصل الخامس:

دور الفيروسات الكمبيوترية في الحروب المستقبلية

يتأكد يوم بعد يوم بأن الفيروسات الكمبيوترية سيكون لها دوراً رئيسياً في تحديد مسارات الحروب المستقبلية، ولقد أدركت القيادات العسكرية في العديد من البلدان هذه الحقيقة، وبدأت تشكل الوحدات العسكرية المتخصصة في مواجهة «الهجومات الفيروسية» كما أنه ترد تقارير حول ظهور أنواع جديدة من الفيروسات بصورة متواصلة ومتجددة على الدوام، وهذه الهجمات الفيروسية تمثل التباشير الأولى للطريقة التي ستسير عليها الحروب المستقبلية، كما سبق وأشرنا إلى الأمر.

والواقع أن اعتماد الفيروسات كأسلحة عسكرية بدأ بالفعل منذ الآن، والمعروف أن الدوائر العسكرية في كل من الولايات المتحدة وروسيا، ومعظم البلدان، المتقدمة تعمل على تطوير انواع جديدة من الفيروسات، وأن استعمال الفيروسات لغايات عسكرية قد بدأ بالفعل منذ أواسط التسعينات على الأقل.

ومن الأمثلة على ذلك أن القوات الاميركية المتمركزة في البوسنة كانت قد عانت في 1996 من فقدان بيانات مخزنة في ذاكرة أجهزتها الكمبيوترية؛ ونتيجة لذلك توقفت بعض هذه الأجهزة عن العمل.

ويقول ضباط مسؤولون بأن البيانات المفقودة لم تكن ذات أهمية حيوية لضمان حسن سير عمليات التجسس الأميركي في البوسنة إلا أنها أجبرت العاملين الاداريين في هذا الجيش على تخصيص مئات الساعات من الجهد المكثف لاكتشاف الفيروسات وتطهير الأنظمة الكمبيوترية منها، مع السعي إلى إعادة تكوين البيانات المفقودة.

وذكرت مصادر الجيش الأميركي بأن الفيروسات التي أصابت الأجهزة الأميركية في البوسنة قد تم ادخالها بواسطة جندي كان يستعمل قرص كمبيوتري مصاب بتلك الفيروسات لدى تحويل المعلومات بين الأجهزة.

وهذه قائمة ببعض أبرز الفيروسات التي أصابت الأجهزة في البوسنة:

- فيروس انتي اكزي (Anti Exe) المعروف أيضاً بفيروس دي 3 (D3). وهو فيروس يصيب ذاكرة الأقراص الصلبة الكمبيوترية ويتسبب بعدة اعطال.

- فيروس كونسبت (Concept) أو فيروس فرانك ماكرو (Franck Macro) ويتسبب بتعطيل بعض التعليمات الكمبيوترية. مثلاً لجهة منع محو بعض البيانات من الذاكرة، وهو ما يتسبب بامتلاء هذه

الذاكرة كلياً وبعدم تمكنها من استيعاب بيانات جديدة.

- فيروس القرد (Monkey) الذي يعطل استعمال القرص الصلب وتتطلب معالجة أثاره إزالة جميع البيانات المخزنة على هذا القرص واستبدال جميع البرامج التشغيلية في الكمبيوتر ببرامج جديدة خالية من الفيروسات.

أما التدابير التي اتخذها الجيش الاميركي لمحاربة تفشي الفيروسات، فإن أبرزها كان:

- وضع موضع متخصص في البرامج المضادة للفيروسات على شبكة الانترنت، على أن يكون هذا الموقع (Site) خاص بالوحدات العسكرية الأميركية العاملة خارج الولايات المتحدة وتتمكن من الحصول على هذه البرامج عن طريق انزالها من الموقع بعد الاتصال به.

- تدريب العسكريين على استعمال البرامج المضادة للفيروسات.

- اجراء عمليات فحص شاملة لجميع الكمبيوترات العسكرية الاميركية للتأكد من خلوها من الفيروسات قبل ارسالها لتستعملها الوحدات العاملة في الخارج.

- وضع احدث البرامج المضادة للفيروسات في هذه الأجهزة.

- ويؤكد الخبراء أن كلفة تنفيذ هذه التوصيات أدنى بكثير من كلفة معالجة الآثار التي يتركها تسريب الفيروسات إلى الأنظمة الكمبيوترية.

بالمقابل، فلقد جرى اتهام الولايات المتحدة في أكثر من مناسبة بأنها تقوم بزرع الفيروسات الكمبيوترية لتعطيل أنظمة خصومها، ومن الأمثلة على ذلك أن الصين كانت اتهمت أميركا بذلك عن طريق التلميح أواسط التسعينات حين نشب خلاف حاد بين واشنطن وبكين، حيث أن الأميركيين كانوا يتهمون الصينيين بالقيام بأعمال قرصنة وبنسخ البرامج الكمبيوترية الاميركية بصورة غير شرعية...

نذكر بأن تطوير الفيروسات الكمبيوترية هو أمر بمتناول أي مبرمج كمبيوتري من الناحية المبدئية، وأن بعض المبرمجين الكمبيوتريين في بعض البلدان مثل بلغاريا والباكستان برعوا في ذلك بصورة خاصة وذلك منذ الثمانينات...

الفصل السادس:

تحديد أعمال القرصنة

لقد حفلت السنوات الماضية بأخبار حول تمكن العديد من المستعملين العاديين للكمبيوتر من الوصول إلى شبكات الكمبيوتر العائدة لوزارات الدفاع في عدد من الدول الكبرى مثل الولايات المتحدة وبريطانيا وغيرها، حيث تمكن هؤلاء المستعملون من الحصول على أسرار حساسة للغاية حول أمور استراتيجية مثل كلمات السر لشن حرب نووية وما شابه ذلك.

ويُعرف هؤلاء المستعملون «بالقراصنة» وهم لا يحصرون نشاطهم في التجسس العسكري وحده، وإنما أيضاً في الشؤون الاقتصادية والتجارية.

ولقد تحولت «القرصنة الكمبيوترية» إلى إحدى الآفات الرئيسية في السنوات الأخيرة، خصوصاً وأن ثمة من يعتبر هذا النشاط نوعاً من أعمال البطولة وشكلاً من أشكال «الثورة العادلة ضد طغيان الأنظمة». وقد تجلت هذه الظاهرة بكل وضوح في السنوات الأخيرة حيث تم تنظيم ندوات ومؤتمرات بصورة علنية حول هذه

الممارسات.

ينتظر أن يتعرض العالم العربي إلى حوادث قرصنة كمبيوترية مكثفة في المستقبل القريب، وخصوصاً مع ارتباط العديد من هذه البلدان بالشبكات الكمبيوترية العالمية مثل شبكة الانترنت(Internet). وأيضاً مع ابرام معاهدات الصلح بين «إسرائيل» وعدد من البلدان العربية.

ونتناول هنا تحديد القرصنة الكمبيوترية مع استعراض عدد من أساليبها ووسائل التصدي لها.

القراصنة ونشاطهم

القراصنة هم مستعملوالكمبيوتر الذين يركزون نشاطهم على الوصول خلسة إلى الأنظمة الكمبيوترية العائدة لغيرهم من دون أن يحق لهم ذلك.

ويتركز عمل القراصنة عادة على:

- ايجاد أرقام الهاتف الهامة التي ترتبط بها الأنظمة الكمبيوترية المستهدفة.

- اكتشاف أنظمة الموديم (التي تربط أنظمة الكمبيوتر بالشبكة الهاتفية) ونقاط الولوج إلى الشبكات الكمبيوترية.

- الحصول على البيانات المخزنة في أجهزة كمبيوترية غير مرتبطة بشبكات عن طريق التقاط الموجات الكهرو مغناطيسية المنبعثة عن هذه الأجهزة عند تشغيلها.

وهذه نبذة عن بعض أبرز أشكال القرصنة.

أ. القرصنة الهاتفية:

المقصود بالقرصنة الهاتفية هنا هو اجراء مكالمات هاتفية دون تسديد أجرة المخابرة، ويتم ذلك باستعمال «علب الكترونية» تحول دون عمل معدات احتساب المخابرة. وهذه العلب هي:

- «علبة سوداء» (Black Box) من شأنها اصدار اشارة مماثلة للاشارة المنبعثة من الجهاز الهاتفي عندما يضع المستعمل السماعة.

- العلبة الزرقاء» (Blue box) وهي تقلد اشارات الموجات المتعددة المستعملة في الاتصالات الهاتفية على المدى البعيد. وهو ما يجعل اشارة القرصنة تبدو وكأنها اشارة لبدالة تحويل الاتصالات.

ب. قرصنة البرامج المحلية:

هذه القرصنة هي كناية عن تجاوز البرامجيات التي توضع للحؤول دون اختلاس نسخ البرامج الكمبيوترية التطبيقية (أي بصورة غير مأذونة). ولقد بدأ ازدهار هذا النوع من القرصنة في الثمانينات في بلغاريا، حيث كان القراصنة يقومون بنسخ البرامج الكمبيوترية الغربية لاعادة تصديرها إلى سائر بلدان أوروبا الشرقية. وكثيراً ما يقوم هؤلاء القراصنة أنفسهم بتطوير فيروسات كمبيوترية جديدة أيضاً.

ومعظم القراصنة من هذه الفئة في البلدان الغربية هم إما تلاميذ ثانويون مولعون بألعاب الفيديو، أو طلاب جامعيون، والصفة

الغالبة عليهم أنهم من المولعين بالكمبيوتر والتكنولوجيا الالكترونية، ويؤمنون بوجوب مجانية استعمال الشبكات الكمبيوترية على أساس أن ذلك يسهل عملية اتصال الناس ويوثق العلاقات الاجتماعية والصداقة بين الأمم والشعوب.

ج ـ مجموعات القراصنة:

ومع انتشار الشبكات الكمبيوترية على نطاق واسع في السنوات الأخيرة، برزت ظاهرة جديدة هي ظاهرة تكتل القراصنة في «نوادي» خاصة لممارسة هذه الهواية أو هذه المهنة. ومكان التقاء هذه النوادي غالباً ما يكون العنوان الالكتروني «لنشرات الكترونية» (Bulletin Boards) على الشبكات (وخصوصاً على شبكة الانترنت) حيث يتم تبادل الأفكار والبرامج والتقنيات الخاصة بممارسة القرصنة.

وبالاضافة إلى هذه الأماكن «الالكترونية» للاجتماع، فإن العديد من هذه الجماعات يمارس نشاطه على نحو علني في عدد من البلدان الغربية، حيث أن لديهم مكاتب شرعية، ويقومون بإصدار كتب ونشرات ومجلات متخصصة في القرصنة، مع الاشارة إلى تعرض العديد من هذه النوادي إلى ملاحقات قانونية.

والحوافز التي تحمل القراصنة على القيام بهذه الأعمال متعددة حيث أن الأهداف «العقائدية» التي سبق الاشارة إليها تخفي عادة أهدافاً أقل مثالية كالرغبة في القيام بأعمال تجسسية أو الاستفادة من خدمات الاتصالات دون تسديد الاكلاف المتوجبة أو مجرد التسلية.

ويقوم بعض القراصنة بهوايتهم هذه من أجل لفت الانتباه اليهم والدخول في ملاك الموظفين المولجين صيانة الأمن الكمبيوتري، أو من أجل الابتزاز في حال حصلوا على معلومات حساسة وسرية، حيث يهددون أصحاب هذه الأسرار بكشفها إذا لم يدفعوا فدية معينة.
وهذه بعض الأساليب التي يلجأ إليها القراصنة من أجل الحصول على المعلومات التي يحتاجونها للتغلغل إلى داخل الشبكات الكمبيوترية:

ـ يتصل القرصان بالجهة المستهدفة (بفتح الدال) مع الادعاء بأنه أحد المسؤولين في هذه الجهة (يعرف عن نفسه باسم أحد المسؤولين).

ـ يتصنعون لكنة معينة عند اجراء الاتصالات الهاتفية من أجل اخفاء أصواتهم الحقيقية.

ـ يدعون أنهم من العاملين في الصيانة الذين يحتاجون إلى معلومات معينة.

ـ يدعون أنهم مؤسسة للابحاث ويطرحون الأسئلة من نوع «أي كمبيوتر تستعملون، أي نظام أمني تريدون» إلخ...

ـ البعض يدعون أنهم يتصلون نيابة عن مسؤول معين (بصفة أمينة السر مثلاً).

ـ ينتحلون شخصية أشخاص معروفين.

ـ بعض القراصنة من النساء يدعين أنهن «زوجة صاحب المعلومات التي تحتاج إلى ملف كمبيوتري وهي أضاعت كلمة المرور»...

ـ انتحال صفة موظف البريد للاستفسار عن الارقام المعتمدة

لاجراء الاتصالات البيانية.

- انتحال صفة موظف ضريبة الدخل للحصول على معلومات مالية (خصوصاً في البلدان التي لا وجود فيها للسرية المصرفية).

- انتحال صفة مسؤول أمن الشبكة للحصول على كلمة المرور الخاصة بالمشترك المقصود.

- ارسال برقيات فاكس بأسماء هيئات تقنية طلباً لبعض المعلومات، حيث أن العديد من الناس يعتقد أن هذه البرقيات حقيقية.

- استعمال شبكات الرد الأوتوماتيكي على الاتصالات لإعادة توجيهها. عن طريق ايهام المتصل بهذه الشبكات بأن رقم الشبكة قد تبدل، وتزويده برقم القراصنة بدل من ذلك.

والطريقة الأفضل لمجابهة عمل القراصنة هي أن يضع المسؤولون عن الأمن الكمبيوتري أنفسهم مكان هؤلاء (أي القراصنة)، بحيث يتمكنون من تعلم كيفية تصرفهم من أجل تطوير وسائل مضادة فعالة. وهذه قائمة ببعض الوسائل التي يمكن اعتمادها لهذه الغاية:

- اعطاء أقل قدر ممكن من المعلومات حول كيفية الدخول إلى الشبكات الكمبيوترية.

- اعتماد أقل قدر ممكن من المعلومات حول كيفية الدخول إلى الشبكات الكمبيوترية.

- اعتماد كلمات مرور معقدة تتألف من أرقام مثلاً، وليس من كلمات شائعة.

- مراقبة نشاط النشرات الكمبيوترية التي تتعاطى المواضيع التي تتناولها الجهة المستهدفة(بفتح الدال) مع محاولة الولوج إلى النشرات الكمبيوترية السرية الخاصة بالقراصنة، ثم استعمال المعلومات التي تجمع بهذه الطريقة لتطوير وسائل حماية فعالة.

- سن أنظمة صارمة جداً لجهة اتلاف الوثائق الحساسة. يحيث يتم اتلافها بصورة لا تترك أي أثر، ثم تدريب الموظفين لكي يرفضوا أي طلب من شأن الاستجابة له خرق الانظمة الامنية الخاصة بالجهة المستهدفة. هذه المعلومات والارشادات التي ذكرناها يصلح العمل بها في الدول الغربية بصورة رئيسية، إلا أن العديد من البلدان العربية بدأت ترتبط بالشبكات الدولية للاتصالات البيانية. والظروف الاقليمية المرتقبة سوف يكون من شأنها ازدياد نشاط القراصنة في الدول العربية من أجل غايات التجسس السياسي والعسكري والاقتصادي في آن، ولذلك من الضروري التصدي ولاستعداد منذ الآن لمواجهة هذا الخطر الجديد واتخاذ الاجراءات المشددة المشدد لمنع استعمال القرصنة في العالم العربي.

الفصل السابع:

بعض حالات القرصنة المعلوماتية على الدوائر الامنية والعسكرية

لقد ملأت وسائل الاعلام في السنوات الأخيرة وما تزال أخبار حول نجاح قراصنة كمبيوتريين من الأفراد العاديين في اختراق الشبكات الكمبيوترية الحساسة الخاصة بالدوائر الأمنية والعسكرية في عدد من الدول القوية، وعلى رأسها الولايات المتحدة، والواقع أن التقنيات المستعملة للقيام بهذه الأعمال لم تكن بالغة التعقيد، وقد استعرضنا بعض هذه التقنيات في فصول سابقة، ويبدو أن حصول هذه الحالات هو الذي حدا بالقيادة الأميركية على أخذ الموضوع بجدية وعلى تشكيل فرق خاصة بالحرب المعلوماتية على النحو الذي رأينا.

وفي هذا الإطار، أفادت وكالة أنظمة المعلومات الدفاعية (Defense Information Systems Agency) في الولايات المتحدة أن مواقع وزارة الدفاع الأميركية تعرضت إلى 250,000 هجوماً معلوماتياً خلال سنة 1995، وأن 65٪ من هذه الهجمات حققت أهدافها وتمكن القراصنة

«المهاجمون» من الحصول على البيانات التي كانوا يريدونها من خلالها.

ولم تكتمل الاحصاءات الخاصة بالسنوات اللاحقةعند كتابة هذه السطور، إلا أنه من المؤكد أن عدد الهجمات على مواقع وزارة الدفاع الأميركية قد ارتفع، وكذلك الأمر في ما يتعلق بنسبة الهجمات الناجحة. ونذكر هنا أن القراصنة المعلوماتيين اليهود هم من بين أبرز من يقوم بقرصنة المواقع الأمنية الأميركية على الانترنت، وأن هذا الأمر يثير امتعاض دوائر وكالة المخابرات المركزية الأميركية سي آي أي، خاصة وأن اليهود لا يتورعون عن بيع الأسرار الأميركية الحساسة إلى اعداء الولايات المتحدة عندما يجدون في ذلك ما يخدم المصلحة اليهودية العليا، وتؤكد عدة مصادر عليمة بأن شرائح هامة من وكالة سي آي أي أخذت تكن العداء لـ «إسرائيل» واليهود لهذه الأسباب (يُراجع بهذا الخصوص كتابنا «الأنظمة الحديثة للمخابرات» للمزيد من التفاصيل).

أما فيما يتعلق بروسيا، فلقد أكد أوليغ غورديفسكي (Oleg Gordievsky)، وهو عميل سابق في وكالة المخابرات السوفياتية «ك جي بي» (KGB) لجأ إلى الغرب بأن 40٪ من ضباط هذا الجهاز على الأقل متورطون في «جرائم معلوماتية» من قبيل القرصنة أو زرع الفيروسات الكمبيوترية.

وأكد أن الوكالة تمكنت في وقت ما من التعرف إلى شيفرة

الاتصـالات السـرية الخـاصـة بـ 68 بلداً، ومنها بلدان مثل الولايات المتحدة وفرنسا وغيرها من الدول الأعضاء في حلف شمالي الأطلسي «الناتو» (NATO).

وأكد غورديفسكي بأن جهاز المخابرات في النظام الروسي الذي خلف الاتحاد السوفياتي السابق مستمر في هذه الممارسات، ويعمل على تطويرها.

وهناك عدة تقارير أخرى تؤكد هذه المعلومات، إلا أنه لا بد من الاشارة إلى أن الحالة الفوضوية التي تتخبط فيها روسيا في نهاية التسعينات تعني أن الدولة الروسية لا تسيطر على الوضع، وأن عصابات القرصنة المعلوماتية الروسية قد تتصرف على نحو جماعات مستقلة في ما بينها وتعمل لحسابها الخاص وليس لحساب الدولة الروسية الغائبة من الناحية العملية. كما حصلت عدة حالات للقرصنة تعرضت لها دوائر الجيش الفرنسي، مع اتهام الفرنسيين للأميركيين بالقيام بهذه الأعمال، علماً أن الأميركيين أيضاً يوجهون اتهامات مماثلة إلى الفرنسيين.

أما في بريطانيا فإن وكالة يونيراس (UNIRAS) هي التي تتولى الافادة عن حوادث القرصنة التي تستهدف أنظمة الكمبيوتر الحكومية، ومعالجة هذه الحوادث ولقد شكلت هذه الوكالة سنة 1992، وصلاحيتها غير محصورة بالأمن المعلوماتي وحده.

والأمر اللافت هو أن هذه الوكالة لم تقر بوجود أية حالة ناجحة

للقرصنة استهدفت الأنظمة الحكومية البريطانية وذلك في الوقت الذي تعترف فيه الولايات المتحدة بحصول ألوف الحوادث الناجمة التي استهدفت أنظمة وزارة الدفاع الأميركية، كما رأينا..

ويعتقد الخبراء بأن هذه النتيجة «الخارقة» يجب أن تقلق البريطانيين بدلاً من أن تطمئنهم حيث أن عدم اكتشاف حوادث القرصنة وزرع الفيروسات ربما يدل فقط على أن هذه الحوادث كانت متقنة إلى درجة أنه لم يتم كشفها، أو أن عملاء «يونيراس» كانوا مهملين لواجباتهم ولم يتنبهوا لها....

هذا، والمعروف أن دوائر الأمن، وكذلك الشركات الخاصة، باتت تستعين حالياً بخدمات قراصنة معلوماتيين لاختبار مستوى سلامة الأنظمة الامنية الكمبيوترية، مع الاشارة إلى أنه تم القاء القبض على العديد من هؤلاء القراصنة في البلدان الغربية، وتم الحكم عليهم بعقوبات سجن تمتد لسنوات طويلة.. وقد تعود قساوة هذه الأحكام إلى «ترهيب» القراصنة من الأفراد لكي لا يعتدوا على الأنظمة الحساسة من جهة و«لترغيبهم» للعمل لحساب الدوائر الحكومية وليس ضدها. من جهة ثانية. وينتظر أن تتحسن الأنظمة الأمنية الكمبيوترية في السنوات القليلة المقبلة، وأن يتقلص دور القراصنة الأفراد نتيجة لذلك؛ إلا أن القرصنة الكمبيوترية سوف تستمر وسيلة رئيسية في العمليات العسكرية المستقبلية.

ملحق

تقنيات أميركية للتسلل إلى أنظمة أعداء الولايات المتحدة

لا تقتصر الأساليب العسكرية الهجومية بواسطة الكمبيوتر على ارسال الفيروسات الكمبيوترية التي تظهر بصورة علنية وتتسبب بتعطيل الأجهزة، بل يمكن أن ترتدي اشكالاً أكثر تستراً، مع التَقَنُّع باتباع سياسات تجارية معتدلة، و السماح ببيع برامج كمبيوترية تكون عادية في الظاهر وتحتوي في الواقع على فيروسات تسمح بالتعرف على الأسرار المخزنة في ذاكرات الكمبيوتر.

ومن الأمثلة على ذلك ما ذكرته مصادر اعلامية عليمة من أن المخططين العسكريين الأميركيين يركزون جهودهم في المرحلة الراهنة (أواخر التسعينات).على تطوير التقنيات التي من شأنها أن تسمح للجيش الأميركي بالتعرف إلى الاتصالات التي يجريها أعداء الولايات المتحدة، وذلك عن طريق ممارسة أعمال القرصنة المعلوماتية وزرع الفيروسات للتسلل إلى مراكز توزيع الاتصالات. (Communications Switching Stations) التابعة لأعداء أميركا.

تتضمن هذه المراكز مسالك (paths) مدمجة لنقل البيانات المطبوعة والصوتية والفيديوية المتبادلة بين القيادة والوحدات العسكرية. وكثيراً ما تعمل هذه المسالك بواسطة الميكروموجات (Microwaves).

ويتم التحكم بالمراكز بواسطة برامج كمبيوترية تعتمد على شيفرة

مـصـدرية (Source code) تحـتـوي على عـدة مـلايين من الخـطوط (Lines) البرامجية. التي يمكن الدخول إليها سراً واستثمارها من قبل العدو عن طريق استـغلال ما يعـرف «بالثغرات الخفيـة» في خطوط الاتصالات.

و«الثغرات الخفية» التي تظهر على هذه الخطوط تتواجد ضمن البيانات المنطقية (Logic data) أو «التعليمات المحصورة» (Suppressed instructions) في الشيفرة المصدرية؛ ويمكن أيضاً وضع برامجية منطقية خاصة على شكل فيروسات كمبيوترية لاختراق برامج الحماية على حركة البيانات. والتعليمات المحصورة كناية عن برامجيات خاصة جرى ادخالها ضمن الشيفرة المصدرية بهدف إزالة الشوائب (Debugging) أو القيام بتجارب على تشغيل برنامج الاتصالات، أو أنها توصيلات اقامتها بعض الدوائر للتجسس على عدد من أقنية الاتصالات. ويمكن أيضاً أن تكون العمليات المحصورة مجرد أخطاء برامجية بسيطة حصلت عند وضع الشيفرة المصدرية. هذا، ولا بد من أن نذكر أن هذه الممارسات ربما لا تكون حديثة العهد، فالمعروف أن الولايات المتحدة مارست سياسة متشددة طوال ثلاثين سنة لمنع تصدير البرامج الكمبيوترية الأميركية المتطورة إلى البلدان التي كانت معادية لها إلا أنها وفي الوقت نفسه سمحت لبعض الشركات الهامة المنتجة للمعدات الدفاعية بتصدير أجهزة كمبيوتر معقدة مزودة ببرامج متطورة إلى شركات نمساوية والمانية، وذلك

رغم أن دوائر المخابرات كانت واثقة من أن تلك الشركات ستعمد إلى إعادة بيعها لدول أوروبا الشرقية. ولقد تبين فيما بعد أن بلدان أوروبا الشرقية قامت بالفعل بتقليد المنتجات الأميركية واستعمال تكنولوجياتها لصنع أسلحة وأنظمة اتصالات خاصة بها.

ويعتقد بعض الأميركيين أن الهدف من هذا التراخي الظاهر في السياسة الاميركية كان التعرف إلى أسرار هذه الدول، ذلك أن الأنظمة الاميركية التي «تسربت» عن طريق الشركات الالمانية والنمساوية كانت تتضمن فيروسات وبرامجيات خاصة سهلت على الأميركيين انجاز نشاطهم التجسسي، والتعرف إلى الاتصالات والأعمال التي تمت بواسطتها. ومن المحتمل أن تكون هذه الفيروسات الأميركية لعبت دوراً كبيراً في التفوق الأميركي على الاتحاد السوفياتي السابق في الحرب الباردة.

الفصل الثامن:

حرب الكمبيوتر بين الولايات المتحدة والصين

لقد كان الخلاف بين الولايات المتحدة والصين الشعبية حول تطبيق وتفسير قوانين واتفاقات حماية حقوق الملكية أحد أبرز التطورات التي طرأت على صعيد العلاقات التجارية. وكان لب الخلاف يدور حول المتاجرة بالأجهزة والأنظمة الكمبيوترية، وانتهت القضية ظاهرياً بأن الصين وافقت على احترام حقوق الملكية الفكرية، إلا أن واشنطن ما تزال تتهم بكين بممارسة القرصنة في حين تقول الصين بأن هذه الادعاءات الاميركية هي بمثابة تدخلاً غير مقبولاً في شؤونها الداخلية.

وليس في تركيز الخلاف على الكمبيوتر غرابة كبيرة إذا ما أدركنا مدى أهمية الكمبيوتر في تقدم الأمم في الوقت الحاضر، مع تعطش الصين إلى بلوغ مرحلة متقدمة على هذا الصعيد، حيث باتت من أكثر بلدان العالم استيراداً للأجهزة الكمبيوترية، وهي تسعى إلى إقامة صناعة قوية لهذه الأجهزة في أراضيها.

القرصنة:

لقد اتهمت واشنطن الصين بقرصنة البرامج الكمبيوترية وبعدم اتخاذ الحكومة أي اجراء لمحاربة هذه الآفة، وترفض الحكومة الصينية هذه التهمة وتتهم واشنطن بإثارة هذه القضية وبتضخيمها لكي يكون لها حجة للتدخل في شؤونها الداخلية. لن تدخل هنا في تفاصيل هذا النزاع ولن نسعى إلى تبين من هو على حق ومن هو مذنب، إلا أنه يجب أن تستوقفنا الأمور التالية، وذلك لأهميتها على الصعيد الاستراتيجي:

- إن واشنطن تثير دائماً قضية الملكية الأدبية في مفاوضاتها التجارية مع البلدان النامية أو الاشتراكية، والسبب في ذلك واضح وهو أن الولايات المتحدة هي المنتجة الأولى للبرامج الكمبيوترية في العالم، وتتخوف من فقدان هذا المركز إذا ما نجحت دول أخرى في تطوير برامج ناجحة ورائجة من الناحية التجارية عن طريق نسخ البرامج الأميركية أو عن طريق تقليدها. وقبل بضع سنوات، نشب خلاف بين الولايات المتحدة والبرازيل حول هذا الموضوع حيث طالبت البرازيل واشنطن بفتح أسواقها أمام برامجها، فرفضت أميركا ذلك بحجة أن البرامج البرازيلية لم تكن سوى نسخة مقلدة من البرامج الأميركية.

كذلك فإن الشركات الأميركية المنتجة للبرامج الكمبيوترية هي الداعمة الأولى للمنظمات الدولية التي تخصصت في محاربة

القرصنة الكمبيوترية مثل منظمة فاست (FAST) أو منظمة بي أس أي (BSA)، وتشجعها في ذلك الحكومة الأميركية.

إلا أن المشكلة هي في اختلاف تحديد مفهوم الملكية الادبية للبرامج الكمبيوترية، حيث تؤكد واشنطن أن الملكية الأدبية تشمل جميع الفقرات الخاصة بالبرامج، مع عدم جواز استعمال أي جزء منها، في حين تؤكد الأطراف الأخرى انه يجوز استعمال بعض أجزاء البرامج بعد تعديلها وفق ما يعرف «بالهندسة المقلوبة» (Reverse Engineering)، أي بمعنى آخر يجوز «الاستيحاء» من برامج سابقة لتطوير برامج جديدة، من دون «أن يعني ذلك أنه يجوز نقل البرامج كما هي. والشركات الصغيرة المنتجة للبرامج الكمبيوترية هي من هذا الرأي أيضاً لخوفها من أن تقع رهينة للشركات الكمبيوترية الأساسية التي ستسعى إلى احتكار جميع حقوق التأليف...

اشارة هنا إلى أن الاتجاه المستقبلي هو للاعتماد على «البرامج الموجهة» (Object Programs)، أي إلى تكوين برامج مكتملة مكونة من عدة برامج فرعية، وإذا ما طبقت النظرية الأميركية القائلة بدعم اعتماد تقنية البرامج الموجهة مع حمايتها وفق المفهوم الاميركي لحماية حقوق التأليف، فسيسهل على الشركات الرئيسية ممارسة احتكار كامل على قطاع البرامج الكمبيوترية.

خلاصة القول أن النزاع بين الولايات المتحدة والصين الشعبية حول الملكية الأدبية للبرامج الكمبيوترية يندرج في اطار أوسع بكثير

من مجرد نزاع تجاري وقانوني بين دولتين، وهو بمثابة وجه من وجوه تضارب النظريات حول ما هي حقوق الملكية الأدبية، وحول ما إذا كان المطلوب هو حماية الاحتكارات أو تشجيع أطراف مستقلة أو دول نامية في الدخول إلى مضمار التكنولوجيا المعلوماتية.

- من ناحية أخرى، فإن الصين الشعبية تعتبر الدولة الوحيدة التي يمكن أن تنافس الولايات المتحدة من الناحية الايديولوجية كمركز استقطاب للدول النامية بعد زوال الاتحاد السوفياتي سنة 1991، خصوصاً وأن الصين لم تتنكر قط للنظرية الاشتراكية على الرغم من اتباعها خط رأسمالي في أكثر من مجال اقتصادي وتجاري.

والمعروف أن تأخر الاتحاد السوفياتي السابق في اللحاق بالدول الغربية في المجال الكمبيوتري كان من بين أبرز الأسباب التي أدت إلى التخلف السوفياتي من الناحية التكنولوجية، وكان ذلك التأخر من دواعي ضعف الاتحاد السوفياتي وفقدان هيبته الدولية وفي النهاية انهياره.

ويعود سبب تخلف السوفيات على الصعيد الكمبيوتري إلى خشية الحكام الشيوعيين من أن يستعمل الكمبيوتر كسلاح في أيدي المعارضين ضد النظام، مثلاً من أجل نشر أفكارهم، ولم يقع الحكام الصينيون في هذا الخطأ الجسيم، بل أنهم يشجعون قيام صناعة قوية في الكمبيوتر بالصين، ويقدمون الحوافز من أجل استقطاب الاستثمارات في هذا المجال بالصين.

ومن المحتمل أن هذا الواقع لا يروق كثيراً للخبراء الاستراتيجيين الاميركيين الذين يفضلون أن تلقى الصين المصير نفسه الذي لاقاه الاتحاد السوفياتي.

إشارة عابرة هنا إلى أن بعض المحللين والخبراء الأميركيين في الشؤون الصينية يتوقعون تفكك الصين إلى سبع كيانات بعد وفاة الحكام الحاليين (والعديد من هؤلاء طاعن في السن) ويؤكدون أن هذا المصير الأسود هو لصالح الولايات المتحدة والدول الغربية...

ومن الطبيعي إذ ذاك أن يسعى الأميركيون إلى محاولة الحد ما أمكن من اكتساب الصين للتكنولوجيا الكمبيوترية. والسؤال هو: هل تنجح أميركا في مخططاتهم هذه ازاء الصين؟

لن نتطرق هنا إلى الناحية السياسية والعسكرية البحتة من الخلاف الصيني الأميركي، أي أننا لن نتطرق إلى مدى جدية خطر تفكك الصين إلى عدة كيانات في المستقبل، وإنما نكتفي بالتطرق إلى الحرب الكمبيوترية: سوف يكون من بالغ الصعوبة على الولايات المتحدة أن تتمكن من منع الصين من تطوير صناعة كمبيوترية قوية، فواشنطن ربما تتمكن من قطع علاقتها التجارية مع بكين،إلا أنها لن تستطيع قطع علاقة الصين باليابان أو بدول أوروبا الغربية، ولن يصعب على الصين استيراد أجهزة وبرامج كمبيوترية من تلك البلدان، خصوصاً وأن الصين قد أقامت منذ الآن أسساً متينة للصناعة الكمبيوترية الخاصة بها.

والسؤال هنا: هل أن هذا سيسمح للصين بمنافسة الصناعة الكمبيوترية الأميركية في المستقبل؟

الجواب هو لا، أقله على المدى القصير، فالصين بحاجة أولاً إلى تلبية متطلبات سوقها الداخلية من الأجهزة والبرامج الكمبيوترية قبل التفكير بغزو أسواق التصدير، ومدى الحاجات الصينية في هذا المجال هائلة، وقد تستطيع الصين منافسة الأميركان في صناعة الأجهزة الكمبيوترية الشخصية. إلا أنه قد يصعب عليها في الوقت الحاضر طرح أنظمة كمبيوترية تنافسية في الفئات الكبيرة والوسيطة من الأجهزة. وكذلك في مجال الأنظمة التشغيلية والبرامج التطبيقية الكمبيوترية، وذلك لافتقارها إلى الخبرة الصناعية والتجارية في هذا المجال. إلا أن الصينيين يتعلمون بسرعة، وقد تنقلب جميع المعطيات رأساً على عقب في السنوات المقبلة... وربما يكون قلق الأميركيين في محله بالنسبة إلى المستقبل.

الفصل التاسع

بعض جوانب الأمن المعلوماتي الخاص بالأفراد

من الطبيعي أن تكون أركان الأمن المعلوماتي الخاصة بالمستعملين الكمبيوتريين العاديين مهزوزة، مادام الخبراء الأمنيين العسكريين لم يتمكنوا حتى الآن من إيجاد حلولاً جدية لمسألة الأمن المعلوماتي العسكري..

ولقد تم تطوير عدة أنظمة أمنية لصيانة أمن وسرية الأنظمة الكمبيوترية الخاصة بالمدنيين وقد تكون أكثرها فعالية هي تلك التي تعتمد على الخصائص البيولوجية لكل فرد، بحيث يتم تخزين خصائص الأشخاص الذين يحق لهم الدخول إلى نظام كمبيوتري معين في ذاكرة هذا النظام، ويُمنع ولوج الأشخاص التي لا تكون خصائصهم مخزنة إلى الكمبيوتر، إلا أن نجاح هذه الطريقة غير مضمون بالنظر إلى امكانية قيام شخص مؤهل بالولوج إلى الكمبيوتر بخيانة الأمانة من ناحية، أو بفتح الكمبيوتر تحت ضغط يمارسه عليه القراصنة بالتهديد أو الابتزاز... كما أن هناك عدة

وسائل تتيح خرق نظام كلمات مرور فضلاً عن خطر الاصابة بالفيروسات المعلوماتية.

ونقدم في ما يلي نبذة حول بعض الحالات النموذجية لخرق الأمن المعلوماتي المدني مع تجاوز أكثر الأنظمة الأمنية تعقيداً وتحصيناً:

- خلافاً لما يعتقده الكثيرون فإن القوانين المرعية الإجراء في معظم البلدان الغربية لا تمنع المبرمجين من تطوير فيروسات كمبيوترية، وإنما تحظر استعمالها بغرض إلحاق الضرر بالغير.

ومن هذه القوانين القانون البريطاني حول سوء استعمال الكمبيوتر (Computer Misuse Act) الذي يصنف عملية «إجراء تعديل غير مسموح به» على نظام كمبيوتري أو على بيانات مخزنة في الكمبيوتر، بأنها تشكل جريمة يعاقب عليها القانون. بيد أن عملية وضع الفيروسات بحد ذاتها ليست ممنوعة، ولا يتم ملاحقة واضعي الفيروسات إلا في حال ثبوت أنهم وضعوا هذه الفيروسات في جهاز كمبيوتر شخص آخر دون أخذ موافقته.

في مطلق الأحوال، يصعب الكشف عن هوية واضعي فيروسات الكمبيوتر بالنظر إلى أن هؤلاء لا يسعون إلى تسجيل اختراعاتهم وحمايتها لجهة حقوق النشر. ولم يتعرض سوى مبرمج بريطاني واحد للملاحقة والإدانة بسبب وضعه فيروساً كمبيوترياً منذ أن تم اصدار القانون حول سوء استعمال الكمبيوتر...

- لا يتطلب اقتراف القرصنة المعلوماتية عن طريق كشف كلمات

السر استعمال أجهزة وبرامج متفوقة بالضرورة، بل أن أجهزة عادية تكفي في احيان كثيرة لذلك.

وتعمد الشركات المتخصصة في الأمن المعلوماتي إلى تشغيل قراصنة كمبيوتريين ليقوموا بمحاولة اختراق شبكات الزبائن، فيتم حينذاك كشف نقاط ضعف هذه الشبكات، وتتولى شركة الأمن المعلوماتي معالجتها. ومن الطرق المعتمدة للتسلل إلى الشبكات أن القرصان يتصل بالجهاز الكمبيوتري المزود لشبكة الطرف المستهدَف(بفتح الدال) بواسطة جهاز كمبيوتري عادي (مثلاً جهاز محمول) عن طريق خطوط للاتصالات الهاتفية. فيقوم الكمبيوتر بعملية «كشف» أو «مسح» الشبكة لتحديد «الثغرات» التي يمكن الدخول إلى الجهاز المزود عن طريقها. وإثر الدخول إلى الجهاز المزود يتم التفتيش عن ملف كلمة السر. وكثيراً ما تكون البيانات التي تتكون منها كلمة السر هذه قد تبعثرت حينها يقوم القرصان بالتفتيش عن ملف كمبيوتري آخر يحتوى على البرنامج المستعمل لاتمام عملية بعثرة البيانات، وبعدها يستعمل القرصان هذا البرنامج لإعادة تجميع بيانات كلمة السر، مع الاستعانة بمعجم لغوي لتحديد الكلمات المختلفة التي يمكن أن يكون صاحب الشبكة قد اعتمدها لاختيار كلمة السر لديه، وبعد إجراء أعمال المقارنة والتجربة والاختبار، يستطيع القرصان كشف كلمة السر بعد ساعتين من العمل فقط ومن ثم يصبح بإمكانه الولوج إلى جميع الملفات المخزنة في

الكمبيوتر المزود (Server).

– تعتبر الأنظمة الأمنية المبنية على التأكد من الخصائص البيولوجية التي ينفرد بها كل إنسان وكل كائن حي (مثل البصمات ومخطط الأوعية الدموية وغيرها)، الأكثر تحصيناً بالنظر إلى صعوبة تقليدها. ولهذا السبب فلقد بدأت تظهر أنظمة من هذا النوع تستعمل للتأكد من هوية مستعملي الأنظمة الكمبيوترية أو آلات صرف النقود الأوتوماتيكي في المصارف وغير ذلك. بيد أن مخاوف جديدة بدأت تظهر وهي نابعة من تطوير العلماء لطريقة الاستنساخ البيولوجي التي توجت في 1997بولادة النعجة «دوللي». والخوف هو أن يصار إلى استنساخ كائنات بشرية على شاكلة أصحاب الخصائص البيولوجية المخزنة في ذاكرات الأنظمة الأمنية، ويستعمل هؤلاء الأشخاص «المستنسخين» ليحلوا مكان صاحب الحق الأساسي، وذلك أنهم يكونون مشتركين معه في جميع الخصائص البيولوجية. بيد أن الخبراء يخففون من وطأة هذه المخاوف وذلك لثلاثة أسباب:

ـ السبب الأول هو أن تقنية الاستنساخ البيولوجي مازالت في مراحلها الأولى وما يزال من السابق لأوانه التكهن بإنعكاساتها على صعيد الأنظمة الأمنية.

– السبب الثاني هو أنه يمكن تطوير أنظمة أمنية مختلطة تعتمد على الخصائص البيولوجية للمستعملين من ناحية وعلى كلمات مرور من ناحية أخرى، بحيث لا يتمكن من عبورها غير صاحب الصفات

البيولوجية «الشرعي» الذي يكون على علم أيضاً «بكلمة المرور» أي أن النظام يكون محصناً من الناحيتين البيولوجية والبيانية معاً، مما يضاعف مدى صعوبة خرقه.

- وأخيراً، وقد يكون هذا هو الأهم، فإن استنساخ كائن حي في مرحلة البلوغ يؤدي في البداية إلى ولادة كائن حي في مرحلة الطفولة. وعليه يجب إنتظار أن يصبح الكائن المستنسخ بالغاً قبل أن تتماثل خصائصه البيولوجية مع خصائص الكائن الذي تم استنساخه وهو ما يستغرق سنوات عديدة....

في مطلق الأحوال فإن عدد الخصائص البيولوجية عند الكائنات الحية لا يحصى ولا يعد، وهذه الخصائص قابلة لأن تتبدل لأسباب غير طبيعية، مثل التعرض لحادث يترك آثاراً على الجسم؛ ويبقى أن يتمكن الكمبيوتر من استيعاب جميع هذه العوامل ويحللها بصورة تتناسب مع شروط ضمان مستويات معينة من الأمن والسرية.

ولا بد من الاشارة إلى أن انتشار شبكة الانترنت أتاح المجال لظهور أنواع جديدة من الثغرات في الأمن الكمبيوتري تمثل بسهولة نشر الفيروسات على نطاق واسع، أو بإمطار المشتركين بتسهيلات البريد الالكتروني ببيانات تافهة تملأ الذاكرة الكمبيوترية وتحول دون استعمالها بطريقة مجدية، فضلاً عن أن الثغرات الأمنية في البريد الالكتروني تسمح بالاطلاع على البيانات المخزنة أو باتلاف الملفات الكمبيوترية الخاصة بصاحب حساب البريد الالكتروني

المستهدف (بفتح الدال).

ولقد تعرضت العديد من برامج البريد الالكتروني لثغرات أمنية في عام 1998، وطرحت بعض البرامج لسد هذه الثغرات، دون التوصل إلى نتائج حاسمة...

ونقدم في الختام عدداً من الإرشادات الأولية من شأنها اتباعها تفادي إصابة الأنظمة الكمبيوترية بالفيروسات إلى حد بعيد. وإذا كانت تلك الإرشادات تبدو بديهية من الناحية المبدئية، فمن المفيد تذكرها وإتباعها بصورة متواصلة:

- وضع برنامج مضاد للفيروسات واستعماله بصورة منتظمة.
- وضع نسخات إحتياطية للملفات البيانية في الكمبيوتر.
- تجديد البرنامج الماسح للفيروسات بصورة منتظمة.
- التأكد من سلامة الملفات والأقراص الكمبيوترية الواردة من مصادر خارجية قبل استعمالها.
- وضع البرنامج الواقي من الفيروسات على قسم التأهيل في القرص الصلب ضمن إجراءات تشغيل الكمبيوتر.
- نزع الأقراص اللينة من السواقة بعد استعمالها لتفادي حصول تأهيلها بصورة طارئة.

ملحق

وزارة الدفاع الأميركية ترفع السرية عن بعض أنظمة التشفير الكمبيوترية

رفعت وكالة الأمن القومي «ان اس ايه» (National Security Agency) (NSA) الأميركية السرية العسكرية عن بعض برامج التشفير المعلوماتي لديها، في صيف 1998 الأمر الذي يفسح المجال أمام استعمال هذه البرامج في الأجهزة الكمبيوترية التجارية.

معروف أن وكالة الأمن القومي مسؤولة عن أقسام تشفير البيانات في الوكالات الحكومية الأميركية، وتعتبر نشاطاتها أكثر أعمال الدولة الأميركية سرية.

الأنظمة التي تم رفع السرية العسكرية عنها هي خوارزمية «كي اكستشاينج الفورتيم» (Key Exchange Algorithm) وخوارزمية «سكيب - جاك». وكان قد تم وضع الخوارزميتين في البطاقات الكمبيوترية من نوع فورتيزا (FORTIZZA Computer Cards) التي تستعملها وزارة الدفاع الأميركية وتتيح هذه الخوارزميات حصر ولوج مستعملي الكمبيوتر من العاملين في الوزارة إلى البيانات المخزنة في الذاكرات المعلوماتية والتي يحق لهم الاطلاع عليها دون غيرها.

تأتي خطوة رفع السرية عن خوارزميات البطاقات في اطار جهود وزارة الدفاع الأميركية الآيلة إلى تحقيق تعاون في ما بين العسكريين والشركات الصناعية الكمبيوترية لتطوير أنظمة خاصة بتعزيز الأمن المعلوماتي بأسعار معقولة، ليستفيد منها القطاع الخاص.

وكان الرئيس الأميركي بيل كلينتون قد أصدر الأمر التنفيذي الرقم 12958 من أجل تشجيع التعاون في ما بين الدوائر الحكومية الأميركية والشركات التجارية في مجالات الأمن الكمبيوتري، ويركز الرئيس الأميركي كثيراً على هذا الموضوع ويعتبره حيوياً لضمان المصالح الأساسية للولايات المتحدة في المستقبل.

كما لا بد في هذا المجال من الاشارة إلى الاتجاه القاضي باستعمال أكبر قدر ممكن من المعدات الكمبيوترية التجارية في المعدات العسكرية، وذلك لأسباب اقتصادية ومن أجل استفادة العسكريين من التحسينات التكنولوجية التي يتم تحقيقها في القطاع المدني لتكنولوجيا المعلومات.

ولقد اعطينا التفاصيل حول تقنيات التشفير الكمبيوتري في كتابنا «الأنظمة الحديثة للمخابرات» لارتباط هذا الموضوع بالنشاطات المخابراتية بالدرجة الأولى.

خاتمة:
مستقبل الحرب المعلوماتية

على الرغم من كل ما تقدم، فإن الخبراء يجمعون على أن الكمبيوتر وحده لا يمكن أن يشكل ذلك السلاح الفتاك الذي يحسم الحروب، وإنما وسيلة تتزايد أهميتها يوماً بعد يوم وتساعد على رجحان كفة أحد الأطراف في نزاع ما. والواقع هو أن أنظمة الكمبيوتر تمثل وسيلة للتجسس ولجمع المعلومات أكثر مما هي اداة مباشرة لممارسة الحرب وقد حصلت أكثر من حادثة على هذا الصعيد لعل أشهرها قضية برنامج بروميس (Promis) الأميركي الذي تم زرعه في الأنظمة الكمبيوترية التي صدرتها الولايات المتحدة إلى عدد من البلدان، وبصورة خاصة إلى البلدان العربية، بحيث يتم ارسال البيانات التي تعالج في الكمبيوتر بواسطة شريحة خاصة.... وأكدت مصادر غربية أن العدو اليهودي «إسرائيل» كان أبرز من استفاد من هذه الشريحة للتعرف على أسرار البلدان العربية، وذلك بفضل العلاقات الوثيقة

القائمة بين اليهود والحكم الأميركي... (يراجع «ملف اللوبي اليهودي في العالم» بشأن نفوذ اللوبي اليهودي على بلدان العالم).

ومن المحتمل أن يكون قد بولغ في عرض مدى نجاح الأميركيين واليهود في قرصنة البيانات الكمبيوترية العربية، بدليل النكسات المتواصلة التي أصيبت بها أجهزة المخابرات اليهودية في نهاية التسعينات، إلا أن الصحيح أيضاً هو ان اختراق الأنظمة الكمبيوترية العربيةناجم بالدرجة الأولى عن التخلف العربي في التكنولوجيا المعلوماتية، وان الشرط الأول للحؤول دون حصول مثل هذه الحالات يكمن في اكتساب استقلالية كاملة في هذا المجال في جميع مراحل انتاج الكمبيوتر اعتباراً من مرحلة التصميم وحتى مرحلة التجميع النهائي.

أما من ناحية الفيروسات الكمبيوترية، فإن خطرها قد ازداد بصورة بالغة كما رأينا مع الانتشار الواسع الذي تعرفه شبكة الانترنت، وهذا لا يعني أبداً أنه يجب الاستغناء عن هذه الشبكة التي تشكل اداة اعلامية فريدة لجمع المعلومات ولنشرها على نطاق عالمي شامل، وإنما لا بد من أن تتخذ الدوائر الامنية والعسكرية اجراءات وقائية من قبيل تخصيص أجهزة كمبيوترية لتطبيقات الانترنت تكون

منفصلة تماماً عن الأجهزة التي يتم فيها تخزين المعلومات السرية والحساسة، مع ضرورة التدقيق في البرامج التي يتم الحصول عليها بواسطة «شبكة الشبكات» للتأكد من خلوها من الفيروسات، ولقد أتينا في كتابنا «الأنظمة الحديثة للمخابرات» على ذكر أبرز أساليب التجسس عن طريق الانترنت.

يبقى أن التقنيات المعلوماتية تتطور يوماً بعد يوم، وذلك إلى درجة باتت الدول المتقدمة تشكل فرقاً عسكرية ينحصر نطاق اختصاصها في الحرب المعلوماتية، وهو ما استعرضناه بشيء من التفاصيل مع الولايات المتحدة. كذلك، فإن البلدان المتقدمة تسعى إلى الاستقلال ذاتياً في مجال التقنيات الكمبيوترية، ومن الأمثلة على ذلك ما ذُكر من أن الدوائر الأمنية الفرنسية نجحت في نزع الشرائح المركبة في أنظمتها الكمبيوترية الأميركية الصنع والتي كانت مخصصة لايصال البيانات المخزنة في هذه الأجهزة إلى دوائر المخابرات الأميركية؛ كما يدرس الفرنسيون إمكانية الاستغناء عن الأنظمة التشغيلية من نوع مايكروسوفت وندوز واستبدالها بأنظمة مستقلة عن الشركات الكبرى مثل نظام لينوكس (Linux) بصورة خاصة...

خلاصة القول أن الكمبيوتر لن يكون بديلاً عن الأسلحة

النارية التقليدية وعن الأساليب العسكرية المعروفة والتي تتمثل بالقيام بالعمليات القتالية الحربية، وإنما سيكون جزءاً لن يتجزأ من ترسانة الأسلحة، وعاملاً حاسماً لتحقيق التفوق، والانتصار في حروب المستقبل.

القسم الثاني:

الأسلحة غير الفتاكة وحروب المستقبل

مقدمة عامة

لقد شهد تاريخ صنع الأسلحة تطورات عديدة يصعب تعدادها على مر العصور، إلا أن ثمة ثابتة أكيدة في هذه التطورات كانت على الدوام العمل على تصميم وصنع أسلحة أكثر فتكاً وذات قدرات تدميرية أقوى من سابقاتها، وقد وصل الأمر إلى حد تصميم وصنع واستعمال القنابل النووية والهيدروجينية، مع العلم بأن المخزون الحالي لهذه الأسلحة يكفي لتفجير الكرة الأرضية بأسرها أكثر من مرة...

بيد أن هذا التصعيد المستمر في قوة التدمير الخاصة بالأسلحة أدى في نهاية المطاف إلى خلق حالة من رفض مبدأ الفتك، مع التخوف من مفاعيل أسلحة الدمار الشامل على الصعد المختلفة من إنسانية، مع تضاعف عدد ضحايا الحروب، واقتصادية، مع تدمير البنى التحتية والمرافق الانتاجية، وبيئية، وقد يكون في ذلك الأمر الأهم، حيث هناك تخوف جدي من أن يؤدي استعمال أسلحة الدمار الشامل إلى زعزعة الموازين البيئية الدقيقة، وفي ذلك ما من شأنه التأثير على مختلف أوجه الحياة في الكرة الأرضية بأسرها وليس فقط في المنطقة التي قد تكون تعرضت للضرب بالأسلحة المدمرة.

من ناحية ثانية، فإن بزوغ عصر الاعلام المرئي والمسموع أدى إلى نشر صور الحروب والمجازر في مختلف أنحاء العالم بواسطة شبكات التلفزيون والانترنت، ولقد بدأ هذا التطور يؤثر على مسار السياسات الدولية؛ ومن الدلائل الأكيدة على هذا الأمر أن صوراً مختارة واردة من يوغسلافيا ورومانيا جعلت الرأي العام في البلدان الغربية ينقلب لينحاز بقوة لمصلحة الطرف «ضحية» المجازر وضد الطرف «السفاح»؛ ولقد تبين في ما بعد بأن العديد من صور المجازر قد جرى تزويرها ومضاعفة مفاعيلها إلا أن ما حفظه المشاهد العادي لتلك المناظر هو أن ثمة فظائع تجري ولا بد من العمل على وقفها؛ وبالفعل، فإن التطورات العسكرية والسياسية في السنوات الأخيرة أدت إلى تدخل قوى عظمى ضد بعض الأطراف (في يوغسلافيا بصورة خاصة) بعد العمل على تهيئة الرأي العام في البلدان المتدخلة (بكسر حرف خ) لتناصر هذا التدخل.

ومن هنا برزت الحاجة عند بعض العسكريين لاستعمال أسلحة تؤدي إلى تحقيق الانتصار العسكري، وإنما دون الفتك بالأرواح وتدمير الممتلكات، أي باستعمال «أسلحة غير فتاكة» (Non- lethal weapons).

وبالفعل تدأب الدوائر المتخصصة في عدد من البلدان المتقدمة على وضع برامج شاملة لتطوير مثل هذه الأسلحة.

كما جرت بعض التجارب الميدانية المحدودة على استعمالها في ساحات القتال. ومن المحتمل أن تكون بلدان الشرق الأوسط أكثر المعنيين

باستعمال ذلك النوع من الأسلحة، خاصة وأن بعض الدراسات الأميركية تحدثت عن مدى ملاءمة الأسلحة غير الفتاكة لمحاربة ثوار الانتفاضة الفلسطينية بصورة فعالة، على سبيل المثال، لاسيما وأن اليهود بدأوا يجدون أنفسهم محرجين بصورة متزايدة ازاء الرأي العام الغربي من جراء ارتكابهم فضائع ومجازر في لبنان وفي فلسطين المحتلة في النصف الثاني من التسعينات..

وينتظر أن ترتدي الأسلحة غير الفتاكة أهمية أساسية في السنوات القليلة المقبلة، وقد تكون لها آثاراً رئيسية لتحديد مسار الأحداث، بما في ذلك أحداث الشرق الأوسط، ولذلك رأينا من المناسب البحث في ماهية تلك الأسلحة مع دارسة أولى أنواعها وأولى تجاربها، ومحاولة معرفة مدى انعكاساتها وفعاليتها الحقيقية في السنوات المقبلة.

الفصل الأول:

أسباب تطوير الأسلحة غير الفتاكة

هناك عدة أسباب تدعو دوائر الدفاع في البلدان الصناعية الرئيسية إلى التخطيط لاستعمال الأسلحة غير الفتاكة في نزاعات المستقبل، وتعود هذه الأسباب إلى اعتبارات عسكرية وسياسية واقتصادية في آن، وإنما ليس إلى اعتبارات انسانية، وذلك على عكس ما قد يتبادر إلى الأذهان للوهلة الأولى.

الاعتبارات العسكرية تكمن بكل بساطة في أن استعمال الأسلحة غير الفتاكة سيكون من شأنه من الناحية المبدئية شل القدرات القتالية للقوات المعادية وبالتالي شل قدراته على الهجوم أو المقاومة، وهو ما يضطره من الناحية المبدئية أيضاً على الاستسلام بسرعة دون التضحية بعدد كبير من الجنود والأسلحة.

أما الاعتبارات السياسية فإنها تعود إلى أن الرأي العام في معظم الدول الصناعية بدأ يرَفض مبدأ الحروب الطويلة الدامية ولم يعد يتحمل التضحيات الكبيرة بالارواح والممتلكات والكلفة الباهظة لتطوير ولصنع الأسلحة التقليدية «الفتاكة». ولعل من

العلامات ذات الدلالة على هذه الحقيقة أن الولايات المتحدة انتخبت سنة 1992 رئيساً لها كان فاراً من الخدمة العسكرية في حرب فيتنام، وهو أمر ما كان بالامكان تصوره في ما مضى؛ كذلك فإن حرب أفغانستان كانت من الأسباب الرئيسية التي أدت إلى انهيار الاتحاد السوفياتي.

أما من الناحية الاقتصادية، فإن استعمال الأسلحة غير الفتاكة يؤدي من الناحية المبدئية إلى تسريع انهاء النزاعات العسكرية وبالتالي إلى التخفيف من النفقات العسكرية، وهو أمر هام حتى بالنسبة إلى دولة مثل الولايات المتحدة التي لم تستطع تحمل وزر حرب الكويت أو عملية الصومال لوحدها بل اضطرت إلى الاستعانة بجميع حلفائها.

ويمكن ايجاز مزايا الاسلحة غير الفتاكة بالتالي:

- هذه الأسلحة تبدو أكثر «انسانية» وهو الأمر الذي يجعلها أكثر قبولاً لدى الرأي العام.

- الأسلحة غير الفتاكة تتيح للقادة العسكريين دراسة الوضع الميداني قبل المباشرة بأعمال القتال، وذلك بالنظر إلى أن شل الأسلحة غير الفتاكة لاسلحة الاعداء من شأنه أن يحمل هؤلاء على التفاوض.

- ثم أنه في حال لم يتجاوب الطرف المعادي مع الدعوات إلى التفاوض بعد استعمال الأسلحة غير الفتاكة، فإن استعمال الأسلحة الفتاكة التقليدية هذه حينها يصبح أمراً أكثر قبولاً عند الرأي العام إياه.

من هنا نرى أن استعمال الأسلحة غير الفتاكة يبدو وكأنه

بمثابة استكمال لاعتماد الأسلحة الفتاكة وليس بديلاً عنها، وذلك على ضوء المستجدات التي أحدثتها التطورات الاعلامية والاقتصادية في السنوات الأخيرة، وخصوصاً على صعيد تزايد أهمية وسائل الاعلام وتأثيرها البالغ على الرأي العام في جميع بلدان العالم.

يبقى أنه ليس هناك من نظرية عسكرية واضحة حول كيفية استعمال الأسلحة غير الفتاكة ، وذلك بالنظر إلى قلة الخبرة ازاءها حتى الآن، و العديد من القادة العسكريين يشككون في فعالية الاسلحة، أو بمدى فعالية الأسلحة، بمعنى أن مفعول هذه الأسلحة قد يكون مهماً جداً عند استعمالها للمرة الأولى، إلا أن العدو سوف يتعلم كيفية التصدي لها من جراء تجربة هذه المرة الأولى، وبالتالي فإن استعمال الأسلحة غير الفتاكة في المرات التالية سوف يفتقد إلى الفعالية، سيما وأن الأسلحة غير الفتاكة لا «تفضي» على الاعداء وبالتالي تتركهم احياء وقادرين استيعاب تجاربهم، كذلك فإن عدم «قضاء» أو «فتك» الاسلحة غير الفتاكة بالاعداء يجعل أرواح الذين يستعملون هذه الأسلحة غير الفتاكة أكثر عرضة للخطر.

وسوف تتبلور جميع هذه المعطيات في حروب السنوات المقبلة ليتبين مدى إمكانية استعمال الأسلحة غير الفتاكة كأداة رئيسية في العمليات العسكرية، أو كمجرد أداة مكملة واضافية للأسلحة الفتاكة التقليدية.

الفصل الثاني:

أبرز الأسلحة غير الفتاكة

يمكن تصنيف الأسلحة غير الفتاكة إلى أربع فئات:

- الأسلحة الموجهة ضد الأشخاص من أجل اعاقة وعرقلة حركة المقاتلين الاعداء.

- الأسلحة أو الأنظمة التي تعيق حركة المركبات وتمنع استعمالها لغايات عسكرية.

- الأسلحة التي تستهدف البنى التحتية للطرف المعادي، من شبكات للاتصالات أو طرق للمواصلات أو محطات توليد الطاقة وغيرها.

- أنظمة الحرب النفسية.

ونقدم فيما يلي لمحة عن بعض أبرز الأسلحة المطروحة للفئات الاربعة وإنما مع التشديد على أن القائمة المستعرضة هنا ليست كاملة، وأنه يتم تطوير أنواع جديدة من هذه الأسلحة في كل يوم، وأن العديد من الأسلحة غير الفتاكة مازالت سرية أو في مرحلة التطوير. إشارة هنا إلى أساليب الحرب الكمبيوترية تدخل ضمن تصنيف «الأسلحة غير الفتاكة»، ونحن تناولناها في القسم الأول من هذا الكتاب.

·أسلحة غير فتاكة تستهدف الأفراد

- أسلحة لبث الأشعة الليزرية في وجه الاعداء، وكان المقصود من هذه الأسلحة في البداية هو العمل على التسبب بالعمى للجنود الاعداء، وتم حظر مثل هذه الأسلحة من الناحية المبدئية بموجب معاهدة دولية أبرمت سنة 1995، بيد أن هذا الأمر لا يعني أبداً التوقف عن تطويرها؛ إشارة هنا إلى أن الأميركيين طوروا أسلحة ليزرية تتسبب بالعمى بصورة «موقتة» وليس «دائمة». ويمكن استعمال الأسلحة الليزرية أيضاً لتعطيل الأسلحة الفردية التي يحملها الجنود الأعداء، وخصوصاً أنظمة التصويب والاستشعار والكاميرات التلفزيونية. ومن الطبيعي أن استعمال الأسلحة الليزرية لا ينحصر بتعطيل أسلحة الأفراد، وإنما يشمل أيضاً تعطيل الأنظمة الموضوعة على المركبات العسكرية، وهو ما يدخلها أيضاً ضمن فئة أنظمة الأسلحة المستهدفة للمركبات.

- أسلحة تطلق مواد كيميائية تتسبب بمشاكل صحية إلى الجنود المستهدفين (بفتح الدال) من قبيل الاستفراغ أو الاسهال، وهو ما يجعلهم غير قادرين على مواصلة العمل القتالي؛ وتدخل القنابل المسيلة للدموع ضمن هذا التضنيف أيضاً.

تجدر الاشارة إلى أن ارتداء أقنعة واقية يحول دون فعالية أسلحة من هذا النوع.

- كذلك فإن رش مواد لزجة على الطرقات لمنع سير جنود عليها يمكن أن يدخل في هذا الاطار مع العلم بأن الأميركيين لجأوا إلى هذا الاسلوب لتغطية انسحابهم من الصومال سنة 1995.

أنظمة تستهدف المركبات

- أسلحة بالموجات ما دون الصوتية ذات التردد المنخفض (Low-

Frequency Infrasound) التي تبث موجات موجهة إلى القوات المعادية لشل تحركاتهم واضعافها.

- أسلحة الكترونية بالميكروموجات ذات الطاقة المتفوقة لتعطيل أنظمة التحكم الالكترونية.

- أسلحة ليزرية لتعطيل أنظمة التوجيه البصرية الخاصة بالمركبات.

- أسلحة كيميائية لجعل المواد التي تصنع بها مركبات العدو (حديد، لدائن) تتآكل وتتصدأ وتتعطل.

- وفي مجال الأسلحة الكيميائية هناك مادة ترش على الطرقات وتجعل الاطارات المطاطية للمركبات تتفتت بسرعة.

- أيضاً وأيضاً في مجال الاسلحة الكيميائية شحن الغام بمادة غازية تتسرب إلى المحركات وتعطلها بصورة فورية.

- أسلحة بيولوجية لنشر جراثيم يكون من شأنها تحويل الوقود السائل إلى مادة لزجة لا يمكن استعمالها.

- تطوير «روبوتات» صغيرة تستعمل لزرع الألغام، أو لزرع الأسلحة غير الفتاكة المذكورة اعلاه في صفوف العدو.

الأسلحة التي تستهدف البنى التحتية

- أسلحة معدنية: قد لا يكون التعبير في محله تماماً، والأسلحة المعدنية المقصودة هنا هي رقائق معدنية خفيفة يقذف بها لتعطيل الخدمات العامة، وقد استعملت هذه الأسلحة في بداية حرب الكويت، حيث زودت صواريخ توماهوك (Tomahawk) بهذه الرقائق وقصفت 28 موقعاً حول العاصمة العراقية بغداد لقطع التيار الكهربائي عنها.

- مدفع الكتروني لتعطيل أجهزة الكمبيوتر:

في هذا المجال ، طورت الهيئات العسكرية المختصة في كل من الولايات المتحدة وبريطانيا مدفعاً من نوع جديد يتميز بأنه يقذف طلقات من الطاقة الكهربائية ذات الكثافة العالية وليس القذائف النارية. ويعرف هذا السلاح بمدفع «الموجات اللاسلكيْة ذات الطاقة العالية «ايتش أي أر أف» (High Energy Radio Frequency, HERF) والهدف من استعماله هو التشويش على الأجهزة الكمبيوترية وتعطيل تشغيلها.

ويقول الخبراء بأن هذا السلاح فعال بصورة خاصة في حال تم توجيهه ليضرب النظم الالكترونية في الطائرات، وتقول بعض المصادر بأن عدداً من حوادث الطيران حصلت بسببه لأن الطائرات المنكوبة كانت تنقل شخصيات سياسية مستهدَفة (بفتح الدال).

كما تتخوف بعض الأوساط من أن تكون منظمات اجرامية قد تمكنت من الحصول على هذه التكنولوجيا ولقد ذكرت بعض الاشاعات بأن عدداً من المصارف الدولية قد تعرضت بالفعل إلى ابتزاز من نوع جديد مفاده بأن على تلك المصارف تسديد مبالغ محددة وآلا تعرضت أجهزتها الكمبيوترية للقصف بأسلحة «ايتش أي أر أف» ولا يمكن تأكيد أو نفي هذه الاشاعات، بالنظر إلى أن المصارف لا تحبذ نشر الاخبار حول مشاكل الابتزاز التي تتعرض لها، وذلك لكي لا يرتعب زبائنها ولا يعودوا مطمئنين إلى سلامة ودائعهم المصرفية إلا أن الأمر الأكيد هو أن أعمال الاجرام والابتزاز في القرن الحادي والعشرين سوف تعتمد على الاسلحة المعلوماتية «غير الفتاكة».

أسلحة الميكروموجات ذات القوة الكبيرة «ايتش بي أم دبليو» (High Power Microwaves Weapons, HPMW)

لقد بدأت جيوش البلدان الصناعية القوية تختبر هذا النوع من الأسلحة مع درس فعاليتها على صعيد ميدان القتال.

هذه الأسلحة تطلق أشعة بالميكروموجات، وهذه الميكروجات تؤدي إلى القضاء على قدرات أجهزة الرادار وأنظمة الاتصالات. وتؤدي الميكروموجات إلى احراق الدارات البيانية المطبوعة (Printed circuits) في الأجهزة الالكترونية، والشرائح الكمبيوترية، مع العلم بأن هذه الدارات والشرائح تستعمل بصورة أساسية مع جميع أنواع المركبات العسكرية من طائرات وسفن ودبابات وسواها. ويؤدي تدمير المكونات الالكترونية والمعلوماتية للمركبات إلى شل قدراتها العملانية بشكل تام. ويمكن اطلاق شحنات الميكروموجات بصورة متواصلة ومن دون توقف، شريطة تأمين الطاقة الكهربائية بطبيعة الحال.

- رش مواد كيميائية تتسبب بتسريع تآكل المعادن المستعملة لصنع أساسات المباني والمنشآت (مثلاً جسر خاضع لسيطرة جيش معادٍ) بحيث يؤدي ذلك إلى انهيار المباني وعدم التمكن من استعمالها.

الأسلحة غير الفتاكة في الحرب النفسية

يصنف بعض الخبراء الأنظمة التي تعتمد في الحرب النفسية بأنها أسلحة غير فتاكة؛ والمقصود هنا بالحرب النفسية ليس بث الدعاية الموجهة للرأي العام في البلدان المعادية، وإنما السيطرة على وسائل الاعلام في تلك البلدان عن طريق الاعتماد على أجهزة بث بقوة بالغة تعمل على موجات الاقنية الاذاعية والتلفزيونية الخاصة بالاعداء مع نشر اخبار خاطئة وكاذبة تبعث الحيرة وتتسبب بالفوضى في صفوف هؤلاء الاعداء. إشارة هنا إلى أن تقنيات التشبيه والتركيب الكمبيوتري

تجعل من الممكن تركيب صورة لرئيس الدولة المعادية وهو في وضع مذل (مثلاً عرض هذا الرئيس وهو يقبل أيدي أعداءه)، ومن ثم بث هذه المشاهد المركبة على الأقنية التي يكون قد تمت السيطرة عليها.

وتقول بعض الانباء بأن الولايات المتحدة كانت قد فكرت باعتماد هذا الاسلوب ضد العراق سنة 1991 ثم عدلت عن الأمر بعد أن أعلن الرئيس العراقي في مؤتمر صحافي عقده قبل نشوب العمليات العسكرية بأن العراق أيقن هذا الاسلوب، وأن للقوات المسلحة العراقية تعليمات واضحة للتصرف في حال كان الاميركيون لجأوا فعلاً إلى هذا الأسلوب...

إلا أنه ليس من المستبعد أن يتم اعتماد هذه الطريقة في المستقبل، مع العلم أن الرد المناسب تقضي بوضع خطة مسبقة للمواجهة مع عدم الاعتماد على البث الاذاعي العام لنشر الاوامر والاخبار الرسمية، وإنما على وسائل لا يستطيع العدو السيطرة عليها، ويمكن أن تبدو بدائية بالمقارنة مع البث الاذاعي، ونقصد بذلك اصدار أوامر مطبوعة أو مكتوبة بخط اليد مع مهرها بخاتم خاص، أو بنظام تعريف يعتمد على الخصائص البيولوجية (يُراجع بخصوص أنظمة التعريف البيولوجية ما ذكرناه في القسم الأول من هذا الكتاب).

هذا، ولا بد من أن نشدد على أن هذه الحالات التي تم فيا اختيار هذه الأسلحة ما تزال نادرة جداً حتى الآن (بداية 1999) إلا أن العمل جار على قدم وساق من أجل المتعرف إلى خصائص هذه الأسلحة ومزاياها من الناحية العسكرية العملية وليس النظرية.

الفصل الثالث:

أبرز برامج الأسلحة غير الفتاكة

لقد بدأ الحديث يتزايد حول الأسلحة غير الفتاكة في بداية التسعينات؛ وجرت أولى النقاشات الجدية حول النظريات العسكرية لاستعمال تلك الأسلحة في الولايات المتحدة في أعقاب حرب الكويت، حيث كان ذُكر بأن الولايات المتحدة قامت باختيار عدد من تلك الأسلحة.

وكانت الدراسات في البداية كناية عن أبحاث قام بها ضباط بصورة مستقلة، إلا أن وزارة الدفاع الأميركية أولت الأمر أهمية كبرى اعتباراً من أواسط التسعينات وتم تخصيص ميزانية بالغة لتطوير الأسلحة غير الفتاكة، وإنما دون حصر استعمال تلك الأسلحة بفرع واحد من القوات المسلحة، أو بنوع واحد من العمليات العسكرية، وإنما للعمل لتشمل هذه الأسلحة جميع جوانب العمل العسكري.

وتعني هذه «الشمولية» أن الأميركيين يولون هذه الأسلحة أهمية كبرى من أجل تحديد استراتيجياتهم المستقبلية، مع العلم أن

استعمالها (أي استعمال الاسلحة غير الفتاكة) انحصر حتى الآن لتأتي مكملة للاسلحة الفتاكة التقليدية وليس بديلة عنها. ويبدو من خلال قراءة الدراسات العسكرية الأميركية أن الميل في المستقبل هو لاستعمال الاسلحة غير الفتاكة عند بدء العمليات العسكرية من أجل تحطيم معنويات الاعداء وحملهم على الاستسلام السريع ومن ثم العودة للاعتماد على الأسلحة الفتاكة التقليدية في حال لم تنجح هذه الطريقة للتغلب على مقاومة الاعداء. اشارة هنا إلى الجانب الاقتصادي لاستعمال الاسلحة غير الفتاكة، حيث أن من شأن عدم تدمير المنشآت المعادية توفير تكاليف اعادة البناء عند انتها ء النزاع.

ويقوم سلاح مشاة البحرية الاميركية «المارينز» (Marines) بالقسم الابرز من اختبارات الاسلحة غير الفتاكة في أميركا.

وتمت مناقشة استعمال الاسلحة غير الفتاكة في اجتماعات حلف شمالي الأطلسي، ويبدو أن الرأي استقر على وجوب استعمال تلك الاسلحة كاستكمال للاسلحة التقليدية وليس كبديل لها، مع التشديد على استعمالها في عمليات حفظ الامن والسلام.

ويبدو أن معظم جيوش البلدان المتقدمة تدرس امكانية استعمال الاسلحة غير الفتاكة، مع العلم بأن ثمة نظرية سائدة عند بعض العسكريين تؤكد أن الأسلحة غير الفتاكة تشكل خطراً على الجيوش التي تعتمدها وذلك على أساس أن جنود القوات المواجهة لمستعملي الأسلحة غير الفتاكة سيكونون مطمئنين إلى أنهم لن يصابوا بأذى،

وهو الأمر الذي يجعلهم أكثر عدوانية، ولذلك يفضل هؤلاء حصر استعمال تلك الأسلحة بالمهام الدفاعية وليس الهجومية، مثلاً من أجل الدفاع عن المراكز والمواقع العسكرية، أو كبديل عن الالغام الارضية التي باتت محظورة بموجب المعاهدات الدولية من الناحية المبدئية.
وسوف تتبلور البرامج الخاصة بالاسلحة غير الفتاكة بصورة تدريجية في السنوات المقبلة مع المباشرة في الاعتماد عليها بمناسبة النزاعات العسكرية.

الفصل الرابع:

سلاح الجو الأميركي يدرس الاعتماد على الاسلحة غير الفتاكة

من المعروف أن النظرية العسكرية الأميركية السائدة في الوقت الحاضر تدعو إلى الاعتماد المكثف على سلاح الجو من أجل القضاء على مقومات قوة أعداء أميركا عن طريق القيام بعمليات مركزة من القصف الجوي، ومن ثم القيام بعمليات برية بعد أن يكون القصف الجوي قد دمر البنى التحتية المعادية، وأدى ذلك إلى جعل العدو (العدو لأميركا بطبيعة الحال...) عاجزاً عن التصدي لعمليات اجتياح برية، ويفضل الأميركيون تأخير تدخل قواهم البرية أطول مدة ممكنة، والحرب المثالية عندهم هي تلك التي يحققون الانتصار فيها دون الحاجة إلى الدخول في أراضي العدو، مع الاكتفاء بعمليات القصف الجوي... ويعود هذا التركيز الأميركي على وجوب تحقيق التفوق الجوي إلى تجربتهم المرة في حروب كوريا في الخمسينات وفييتنام خلال الستينات وأوائل السبعينات، وإلى حد ما إلى عملية تدخلهم في الصومال أوائل التسعينات.

ولقد تجلت النظرية «الجوية» الأميركية في حرب الكويت سنة 1991، وفي حرب كوسوفو سنة 1999.

ومن الناحية المبدئية، فإن طبيعة العمليات العسكرية بالقصف الجوي لا تتناسب كثيراً مع استعمال الأسلحة غير الفتاكة، حيث أن المطلوب من عمليات القصف الجوي هو الحاق أكبر قدر ممكن من الخسائر بالاعداء، على أن تكون تلك الخسائر بالارواح وبالممتلكات في آن سواء...

ومع ذلك، فإن قيادة سلاح الجو الاميركي تدرس بعناية فائقة الاعتماد على الاسلحة غير الفتاكة في السنوات الاولى من القرن الحادي والعشرين.

ويتطلع القادة الجويون الاميركيون لان تستهدف الاسلحة غير الفتاكة التي يتم اطلاق قذائفها بواسطة الطائرات الافراد وليس البنى التحتية، بمعنى أن تؤدي هذه القذائف غير الفتاكة إلى جعل الافراد التي تصيبهم عاجزين عن القيام بحركات عدوانية وذلك لمدة محدودة، ومن دون أن يؤدي ذلك إلى الحاق اصابات دائمة لهم، أو أن تتسبب بوفاتهم.

ومن الناحية التقنية، فإن الاسلحة غير الفتاكة المختارة لهذه العمليات هي اطلاق نبضات كهربائية ذات قوة عالية، وأجهزة تبث ميكروموجات ذات قوة عالية.

كما يفكر سلاح الجو الاميركي باستعمال قذائف تقليدية، وانما مع

استبدال الشحنات النارية التقليدية فيها بشحنات غير فتاكة، مع مواصلة الاعتماد على أنظمة التوجيه الدقيقة.

أما أبرز العمليات التي يجب أن تستعمل فيها تلك الاسلحة الملقاة جواً فانها عمليات التصدي للتظاهرات أو لاعمال الشغب التي قد تستهدف السفارات والمصالح الاميركية في الخارج، بحيث يتم ابعاد جماعات تقوم بمهاجمة تلك المصالح بعد قصفها بأسلحة غير فتاكه ويسمح هذا الامر باخراج العاملين فيها (أي في المباني الاميركية التي تتعرض للهجوم) بواسطة طوافات...

كما أن سلاح الجو الاميركي قد يفكر باستعمال تلك الأسلحة في عمليات حربية «ميدانية»، بحيث أن «تحييد» الجنود الاعداء المواجهين لقوات أميركية (من دون قتلهم)يكون بمثابة توطئة لعملية تقدم برية تنفذها هذه القوات...

في مطلق الاحوال، فان الشرط الاساسي والضروري لتتحقق تلك النظريات هو أن تتمتع الولايات المتحدة بتفوق جوي واضح على أعدائها، وهو أمر كان متوفر لها في نهاية تسعينات القرن العشرين، (وذلك يعود بالدرجة الاولى إلى وقوع روسيا في حالة من الفوضى السياسية والاقتصادية أدت إلى تأخر بالغ لديها لتطوير أنظمة أسلحتها) ولكنه لن يستمر إلى ما لا نهاية...

يبقى أن أطرافاً غير الولايات المتحدة تدرس أيضاً الامكانات العملية لاستعمال الاسلحة غير الفتاكة الملقاة بها من الجو.

الفصل الخامس:

التجارب الأولى لاستعمال الأسلحه غير الفتاكة

قد يكون أول من استعمل الاسلحة غير الفتاكة بصورة فعالة هم ثوار الانتفاضة الفلسطينية عندما قاموا بزرع «فيروس القدس» الذي كاد يقضي على الشبكات الكمبيوترية الخاصة بجامعات الكيان اليهودي «اسرائيل» في 1988 (يراجع بهذا الخصوص كتابنا «حرب الكمبيوتر في فلسطين»).

بالمقابل، فلقد أفادت مصادر غير مؤكدة (حيث كذبتها بعض الأوساط الأميركية نفسها) بأن العراق كان ضحية فيروس كمبيوتري تمكنِ الأميركيون من زرعه في الانظمة المعلوماتية الخاصة بوزارة الدفاع العراقية قبيل اندلاع حرب الكويت، وكان ذُكر بأن هذه الفيروسات سُربت إلى الأنظمة العراقية بواسطة طابعات تم استيرادها عن طريق بلد أوروبي غربي...

الأمر الأكيد هو أن أسلحة غير فتاكة استعملت في حرب الخليج، وأبرزها :

- تزويد الرؤس الحربية لصواريخ توماهوك (Tomahawk) بأسلاك مطلية ورفيعة مصممة لاختراق شبكات الاسلاك الكهربائية المحيطة بالبوابات الخارجية (outdoor electrical grids)، ولقد استعملت 12 من هذه الصواريخ في الساعات الأولى من عمليات «عاصفة الصحراء».

كما أن لدى سلاح الجو الأميركي نوع خاص من نظام توزيع الذخائر يقوم برش سحابة من الألياف الكربونية المنمنة (cloud of minute carbon fibers) تغلف الهوائيات والمعدات الكهربائية المختلفة وتجعلها غير صالحة للاستعمال إلى أن يتم تنظيفها بصورة كاملة. ولم يتم اختبار هذا النظام في عملية عسكرية حتى الآن (أول 1999).

كما أن بعض المصادر العسكرية كان قد أفاد بأن الأميركيين كانوا قد نشروا في حرب الخليج عربتين مدرعتين مزودتين بنماذج اختبارية مخصصة لكشف أنظمة الاستشعار (sensors) العراقية وتعميتها، إلا أنه لم يتسنَّ استعمالها في العمليات العسكرية.

من ناحية ثانية، رش الأميركيون مادة لزجة على الأرض عندما انسحبوا من الصومال سنة 1995 من أجل منع الصوماليين من ملاحقتهم، وقد نجحت هذه العملية بصورة جزئية، إذ أدت بالفعل إلى ابعاد الصوماليين بعض الوقت إلا أن هؤلاء (أي الصوماليين)

ردوا بسرعة باطلاق النار على الاميركيين المنسحبين مما اضطر هؤلاء إلى الرد بالمثل، فتحولت العملية إذ ذاك إلى تبادل تقليدي للرشقات النارية.

واستعملت أسلحة غير فتاكة في عمليات فصل القوات التي جرت في البوسنة وفي بعض المناطق الأخرى التي تعمل فيها قوات «تحفظ السلام».

ومن الأمثلة الأخرى على التجارب الفعلية لاستعمال الاسلحة غير الفتاكة:

- قام سلاح الجو الأميركي باختبار مولدات للميكروموجات بقوة كهربائية عالية لتأمين الاتصالات، وتم تركيب هذه المولدات على صواريخ تطلق جواً، وكانت التجربة ناجحة مع حصول بعض المشاكل لضبط مدى ونطاق البث.

- بدأ استعمال أسلحة ليزرية مخصصة للتشويش على المعدات الألكترونية في الطائرات المعادية وتعطيلها. ويعرف هذا السلاح بـ «واي أيه ال ـ 1 ايه» (YAL- 1A) ويجري تحسينه حالياً لكي يمكن استعماله لتعطيل المعدات الالكترونية في المواقع البرية للدفاع الجوي.

هذا، ولقد اختبر الباحثون جهازاً ليزرياً موصولاً بمولد للأشعلة الجزيئية. (Particle beam generator) ويقوم هذا المولد بتشتيت أي عائق قد يعترض مسار الشعاع الليزري (مثلاً الغيوم

أو الدخان)، وهكذا يستطيع الشعاع الليزري بلوغ هدفه بسهولة وبصورة مباشرة.

ومن المؤكد أنه تم اختبار أنظمة أخرى من دون أن يتم الاعلان عنها، وسوف تتوضح الحقائق بصورة تدريجية خلال السنوات الأولى من القرن الحادي والعشرين.

الفصل السادس:

احتمالات استعمال الأسلحة غير الفتاكة في منطقة الشرق الأوسط

تحتل منطقة الشرق الأوسط مكانة بارزة في المخططات الاستراتيجية للقوى العظمى، وذلك بالنظر إلى الموقع الجغرافي المميز لهذه المنطقة، بين قارات افريقيا وآسيا وأوروبا، وإلى ثروتها النفطية، وأيضاً إلى التوتر الدائم الذي أوجده زرع الكيان اليهودي «اسرائيل» كورم سرطاني في فلسطين.

وفي هذا المجال، تستعد «الولايات المتحدة» منذ هذه اللحظة للحروب المرتقبة في منطقة الشرق الأوسط، وذلك عن طريق درس امكانات نظم الأسلحة الاميركية الجديدة التي يتم تطويرها حالياً لتدخل الخدمة الفعلية في العقد الأول من القرن الحادي والعشرين.

والأمر البارز هو أن وزارة الدفاع الأميركية تركز جهودها على اختبار الفاعلية المرتقبة لهذه النظم على مسرح عمليات منطقة الشرق الأوسط، وليس على مسرح العمليات في القارة الأوروبية كما كان معهوداً في السابق، وهذا الأمر يعني أن الشرق الأوسط بات الآن

المنطقة الأكثر حيوية بالنسبة إلى الولايات المتحدة، وأسباب ذلك اقتصادية، بالنظر إلى الثروة النفطية، وسياسية، بالنظر إلى ضغط اللوبي اليهودي لتتدخل أميركا مباشرة من أجل نصرة الكيان الصهيوني «إسرائيل».

وأفادت مصادر صحافية أميركية متخصصة بأن وزارة الدفاع الأميركية أجرت في نهاية 1996 «مناورة كمبيوترية» لاختبار فعالية نظم الأسلحة المستقبلية، والمناورة الكمبيوترية تعني أنه يتم وضع المعطيات المختلفة المتعلقة بخصائص الأسلحة الجديدة، ومنها أسلحة غير فتاكة، والعوامل العسكرية المختلفة داخل ذاكرة الكمبيوتر تتم غربلتها ومعالجتها، ويتصرف عدد من الاختصاصيين مع هذه المعطيات «الكمبيوترية» ليقودوا «العمليات الحربية».

ساحة مسرح المعركة

ولقد تمت المناورة في القاعدة الجوية ماكسويل بولاية الاباما (Maxwell Airforce Base, Alabama) وذلك تحت اشراف المختبر الكمبيوتري الخاص بسلاح الجو الأميركي والمعروف بـ «ساحة مسرح المعركة» (Theater Battle Arena) ومركزه في وزارة الدفاع الاميركية. وقد أجريت التطبيقات التشبيهية (Simulation) في المناورة على 40 جهاز سوبر كمبيوتر من انتاج شركة سيليكون غرافيكس (Silicon Graphics).

وكان موضوع المناورة «نشوب حرب في منطقة الشرق الأوسط

في العام 2010 مع حصول وضع «يفرض تدخل الجيش الأميركي» ومع التركيز على درس امكانات نظم الأسلحة التالية:

- المدفع الليزري المحمول جواً أي بي ال، (Ai, ABL, Brome Leaser,).
- الطائرة المقاتلة أف ـ 22 (F-22).
- نظام الدفاع على مسرح عمليات ذات ارتفاع عال «تاد» (Theater high Altitude Area Thaad defense).
- السفينة الترسانة (Arsenal Ship).

وقد اشتركت في المناورة عدة فرق كمبيوترية مثلت القوات المحاربة، حيث مثلت «فرق زرقاء» القوات الأميركية (Blue Teams) تقابلها «فرق حمراء» (Red Teams) رمزت إلى القوات العربية الواقفة في وجه الأميركان في الحرب.

وقضت قواعد المناورة بأن «تجرب» كل فرقة أنماطاً مختلفة من أساليب ممارسة اعمال القتال وذلك من أجل دراسة أكبر عدد ممكن من الاحتمالات مع كيفية مواجهتها من الناحية العملية. ولقد تألف كل «فريق أزرق» من ضباط من أعلى الرتب خدموا في مختلف فروع الجيش الأميركي (مشاة، جو، بحرية) في حين تألفت «الفرق الحمراء» من أشخاص عملوا في دوائر الأمن والمخابرات ولهم خبرات متعددة الأوجه في التجسس على الدول العربية والقيام بعمليات تخريبية فيها. وقد افترض برنامج المناورة بأن «الفرق الحمراء» قادرة على استعمال الصواريخ الباليستية وأسلحة الدمار الشامل والأسلحة

التقليدية المعروفة.

وقد لحظت المناورة أيضاً وجود «فرق خضراء» (Green Teams) تمثل أطرافاً دولية تقف على الحياد عند نشوب الحرب ثم تضطر إلى التورط في القتال.

أما سيناريو هذه الحرب، فهو أن تبادر «الفرق الحمراء» إلى شن العمليات العسكرية بصورة خاطفة لا تترك أمام «الفرق الزرقاء» إلا وقتاً ضئيلاً للاستعداد القتالي.

وقد تضمنت «العمليات» أربع مراحل مختلفة:

- المرحلة السابقة لنشوب القتال، ولا تزيد مدتها على أربعة أيام.
- المرحلة الثانية، وتغطي الساعتين الاوليتين لنشوب القتال.
- المرحلة الثالثة، وتتناول العمليات الحربية.
- المرحلة الرابعة، وتغطي نهاية الحرب، وتستمر لثلاثة أسابيع.

- ولقد أفادت مصادر عسكرية أميركية بأن أبرز الدروس التي تم استخلاصها من «المناورة» كانت التالية:

- بأن الحفاظ على وحدة تحالف عسكري مشكل بين عدة بلدان هو من الأمور البالغة الصعوبة، وبأن «القوات الحمراء» سوف تبذل أقصى جهودها من أجل اضعاف مثل هذا التحالف والعمل على تفكيكه.

- بأن امتلاك قوة عربية لأسلحة دمار شامل (نووي، بيولوجي، كيميائي) يشكل تهديداً خطيراً، أياً كانت الأسلحة الأخرى المتوفرة لدى

لدى هذه القوة.

ـ بأن النظم المستقبلية للجيش الأميركي «برهنت» على فعاليتها إذا ما تمّ استعمالها بصورة منسقة وجماعية.

ـ بأن على القوات «الزرقاء» أن تتصرف بصورة سريعة وغير منظمة لتتمكن من الرد على هجوم «أحمر» مباغت، وقد أبرزت «المناورة» أهمية دور العمليات اللوجستية، للاستعداد للحرب، وسوف تتركز المناورات المقبلة على هذا الجانب.

ـ المناورة أثبتت ضرورة ادماج استعمال أنظمة الدفاع الخاصة بتغطية منطقة بكاملها (Area defense weapons) أو نقطة محددة (point defense weapons) لمواجهة الصواريخ الباليستية. ولقد استعملت نظم (أي بي ال) لتواجه تلك الصواريخ في المرحلة الأولى من «الحرب» وليس لضرب الاقمار الصناعية أو طائرات كما هو مقرر لها في الأساس.

هذا، ويبقى أن نقول أن استعمال الكمبيوتر لدارسة أسلحة لم يتم اختبارها بعد على أرض الواقع هو أمر مفيد بلا ريب إلا أنه لا يغني أبداً عن اجراء مناورات حقيقية بالذخائر الحية، وأن سر الانتصار في الحروب يكمن في النهاية في كيفية ابتكار خطط ووسائل حربية جديدة لا يتوقعها العدو ولا يكون مستعداً لمواجهتها.

والمهم هو أن هذه المناورة والتحليل الأميركي لنتائجها أظهرت «رعب» الأميركيين من امتلاك العرب لأسلحة للدمار الشامل، والواقع

أن هذا «الرعب» نابع من علاقة التحالف الاستراتيجي الذي يربط بين الولايات المتحدة و«إسرائيل» وهو التحالف الذي تمكن يهود أميركا من فرضه على الاميركان (حيث من الطبيعي والمنطقي من الناحية الموضوعية أن مصلحة الولايات المتحدة هي مع العرب وليس مع اليهود...)، وهو بالتالي رعب يهودي وليس أميركي من امتلاك العرب لأسلحة الدمار الشامل.

صحيح أن «اسرائيل» تمتلك أسلحة للدمار الشامل، لا أن استعمال هذه الأسلحة ضد العواصم العربية سيكون بمثابة ضرب على طريقة «عليّ وعلى أعدائي»، وذلك بالنظر إلى قرب فلسطين المحتلة من البلدان العربية التي قد تكون مستهدفة (فتح الدال)، وذلك باعتراف رئيس أركان جيش اليهود أمنون شاحاك في تصريح كان أدلى به سنة 1997 حيث كان ذكر أن «إسرائيل» لا يمكنها بحال من الاحوال الرد على هجوم سوري بالقنبلة النووية لأن دمشق تبعد 60 ميلاً عن تل أبيب مما يجعل العملية «سلاحاً ذا حدين».

من هنا نرى أهمية الأسلحة غير الفتاكة بالنسبة إلى اليهود وحلفائهم، وقد أوردنا أمثلة عن استعمال مبكر لتلك الاسلحة في العراق والصومال، كما أنه لا بد من الاشارة إلى أن أحد أهم الكتب لأميركية حول حروب المستقبل، وهو كتاب «حرب وحرب مضادة».(war & anti-war) أعطى كمثال على حسن استعمال الاسلحة غير الفتاكة ملاءمة استعمالها لتفريق التظاهرات الفلسطينية في

مدينة القدس.

وهكذا يتبين مدى أهمية الاسلحة غير الفتاكة في النزاعات المقبلة بمنطقة الشرق الأوسط مع ضرورة استعداد البلدان العربية للتصدي لتلك الأسلحة، وذلك عن طريق تطوير أنواع عربية خاصة من هذا النوع الجديدة من أدوات الحروب في المستقبل.

الفصل السابع:

الأسلحة غير الفتاكة وأسلحة الدمار الشامل

لقد رأينا أن أحد أبرز البواعث على استعمال الاسلحة غير الفتاكة هو العمل على تقصير أمد الحروب العسكرية، مع الحد من تكاليفها. والواقع أن الأسلحة غير الفتاكة تلتقي في ذلك مع الهدف من استعمال أسلحة الدمار الشامل من نووية وكيميائية وبيولوجية، إلا أن الفارق بين الاثنين هو أولاً أن أسلحة الدمار الشامل هي أسلحة «فتاكة» و«مدمرة تؤدي إلى قتل الاعداء وتدمير معداته، والسبب الثاني، والأهم هو أن لأسلحة الدمار الشامل انعكاسات بيئية يمكن أن تؤثر على الجيوش التي تعتمدها نفسها، ذلك أن تفجير الاسلحة النووية يؤدي إلى بث الاشعاعات وإلى تدمير البيئة، وهو الأمر الذي يؤثر على الطبقة الهوائية في الكرة الأرضية بأسرها كذلك فإن مفاعيل نشر الغازات الكيميائية تحول دون تمكن القوات التي تكون أقدمت على بث هذه الغازات من الدخول إلى المنطقة المعادية التي تكون أصيبت بالغاز لمدة طويلة، فضلاً عن أن ارتداء ملابس وتجهيزات مضادة للمواد الغازية يمكن بدوره أن يسفر عن مضاعفات صحية خطيرة على من يتزود بهذه الملابس والتجهيزات، كما حصل مع الجنود الغربيين الذين اشتركوا في حرب

الكويت وفق ما جاء في جميع التقارير.

أما بالنسبة إلى الأسلحة البيولوجية، أي لنشر الامراض السارية في صفوف الاعداء، فإن السيطرة على هذا النوع من الأمراض وعلى تفشيها أمر بالغ الصعوبة، وبالتالي يمكن أن يؤدي ذلك إلى تفشي الأمراض عند الذين يكونون قد قاموا بنشرها في الأساس.

من هنا نفهم أن «تحييد» أسلحة الدمار الشامل هو من النتائج التي يأمل الداعون إلى اعتماد تلك الأسلحة بالتوصل إليها، (مثلاً، عن طريق خربطة الأنظمة التي تتحكم باطلاق الاسلحة النووية بواسطة فيروس كمبيوتري أو باصابة تلك الانظمة بشحنة كهرومغناطيسية قوية).

بيد أنه يمكن أيضاً أن يتم دمج الأسلحة غير الفتاكة مع أسلحة الدمار الشامل، بحيث تستعمل أسلحة الدمار الشامل من أجل تدمير بنى تحتية دون الحاق خسائر بالأرواح، وفي هذا المجال، يؤكد العديد من الخبراء الاستراتيجيين بأن شبكات نقل الطاقة الكهربائية التجارية في الولايات المتحدة يمكن أن تكون معرضة للتعطيل بصورة شبه كاملة في حال جرى تفجير شحنة نووية في الفضاء الخارجي على ارتفاع 250 ميلاً فوق مناطق وسط الولايات المتحدة. والسبب في ذلك هو أن التفجير النووي «الفضائي» في هذه الحالة يولد نبضة كهرومغناطيسية (Electro Magnetic Pulse) تبلغ قوتها حدا يجعلها تقطع التيار الكهربائي عن 48 ولاية أميركية (مع استبعاد ولايتي الاسكا وهاواي البعيدتين عن وسط الولايات المتحدة).

لقد تباحث خبراء قانونيون وعسكريون أميركيون في النتائج المترتبة على حصول مثل هذا التهديد في حلقة دراسية خاصة عقدت

برعاية البيت الأبيض سنة 1997.

وتخوف المنتدون من أن تتمكن دولة معادية للولايات المتحدة أو جماعة ارهابية من شن هجوم كهرومغناطيسي يؤدي إلى شل شبكات الاتصالات ومحطات توليد الطاقة والأنظمة الكهربائية في الالات والمركبات، وكذلك تعطيل الاقمار الصناعية على مدارات منخفضة، وتسبب كل هذا بتعطيل كل المرافق الاقتصادية بأميركا على نحو شبه كامل.

من الناحية التقنية، فان اطلاق النبضة الكهرومغناطيسية يدوم مدة لا تزيد عن بعض اجزاء المليون من الثانية، ومفاعيلها مماثلة لتلك الخاصة بالصواعق (Lightning strike)، ودون أن ينتج عنها دمار مباشر - أو قتل أشخاص، ولذلك يمكن تصنيفها في خانة الاسلحة غير الفتاكة.

أما من الناحية القانونية والديبلوماسية، فان تشريعات القانون الدولي لا تنص على أن الهجمات بالنبضات الكهرومغناطيسية تدخل في خانة الأعمال الحربية، وبالتالي لا يحق لدولة تتعرض لهجوم من هذا النوع أن ترد بشن عمليات عسكرية من الناحية المبدئية. ويقول الخبراء الاميركيون بأن الدارات الالكترونية الحديثة التي حلت مكان تكنولوجيا الانابيب الفراغية (Vacuum tubes) القديمة هي أكثر عرضة للتلف نتيجة اطلاق نبضة كهرومغناطيسية، ذلك أن الأنابيب الفراغية كانت محصنة و«مصفحة» لمواجهة التعرض لنبضات ذات نسبة فولتية عالية.

كما ارتفعت نسبة امكانية تعرض الجيش الاميركي لحالة من شل امكاناته الحركية والقتالية بسبب اعتماده المتزايد على أجهزة الكترونية ومعلوماتية مدنية وغير معدلة لتتلاءم مع متطلبات الحرب الالكترونية

الحديثة.

لقد أوصى تقرير قدمته وزارة الدفاع الأميركية بأن يتم تخصيص ميزانية خاصة لدراسة السبل الآيلة إلى تحصين المكونات الالكترونية العسكرية من خطر التعرض لهجوم باطلاق نبضات كهرومغناطيسية، مع المطالبة بدراسة هذه السبل في المراحل الأولى لتطوير الأنظمة الجديدة.

كما أن هناك عدة سيناريوهات أخرى محتملة للدمج بين استعمال أسلحة الدمار الشامل مع «الحرب غير الفتاكة» والسؤال هو إلى أي مدى يمكن أن تحول فيه الأسلحة غير الفتاكة دون استعمال أسلحة الدمار الشامل.

الخاتمة

الحقيقة هي أن تطلع الانسان لكسب الحروب من دون ممارسة أعمال القتال والتعرض لخطر الابادة ليس بالأمر الجديد، حيث أن المفكر الاستراتيجي الصيني صن تزو ذكر في كتاب له يعود إلى ما يقارب 2500 عاماً من الآن «بأن أفضل ما يمكن أن يصبو إليه المقاتل هو تحطيم مقاومة العدو دون قتال». والواقع أن التاريخ القديم والحديث يعطي أكثر من مثال يبين كيف أن طرفاً ما تمكن من الفوز على الرغم من أنه كان في وضع عسكري أضعف من عدوه، وذلك بمجرد استغلاله لاساليب الحرب النفسية مع تحطيم معنويات هذا العدو.

إن للاسلحة غير الفتاكة دور أساسي في تحقيق التفوق عن طريق تحطيم معنويات الاعداء، بيد أن الاسلحة غير الفتاكة لن تحل وحدها مكان الاسلحة التقليدية، كما أن استعمال التكنولوجيات المتقدمة ليس وحده الكفيل بتحقيق التفوق، حيث تمكنت بعض الجماعات الصومالية من التفوق على الاميركيين مع استعمال أنظمة بدائية للاتصالات في سنة 1995 (من قبيل ارسال الاشارات الدخانية

وتفادي استعمال الهاتف لتجنب خطر التنصت عليها)، كما أن بعض المناورات الاميركية بينت أن الاعتماد المكثف على النظم الالكترونية والمعلوماتية يعيق الجنود ويبطىء من سرعة حركتهم بالمقارنة مع أسلحة نارية بسيطة...

والأمر اللافت هو أن تطوير أنواع عديدة من الأسلحة غير الفتاكة لا يتطلب بالضرورة صرف مبالغ طائلة، ويمكن أن يكون بمتناول بلدان فقيرة، أو حتى بمتناول منظمات مستقلة تعمل خارج اطار الدول وهذه الحقيقة من شأنها أن تبدل أموراً عديدة وأن تقلب موازين القوى للسنوات المقبلة، بحيث أن مراكز النفوذ في طريقها لأن تتغير بصورة رئيسية خلال القرن الحادي والعشرين، وذلك بالتوازي مع تبدل أنماط القتال والاعتماد على أنواع جديدة وثورية من الاسلحة.

وسيكون للاسلحة غير الفتاكة دوراً أساسياً في تحقق هذا التبدل، كما أنها قد تكون هي الراجحة لتحديد مصير الأمم في حروب المستقبل.

أبرز المصادر

● **دوريات عربية:**

- مجلة البناء.
- مطبوعات دار الصياد.
- صحيفة الثورة.
- صحيفة الديار.
- مجله فلسطين الثورة.
- صحيفة الكفاح العدبي.
- صحيفة الشرق.

● **دوريات أجنبية:**

- صحيفة ديفانس نيوز (Defense News) الاميركية.
- مجلة أفياشن ويك (Aviation Week) الأميركية.
- مجلة جاينز ويكلي (Jane's Defense Weekly) البريطانية.
- مجلة الاكسبرس (L'express) الفرنسية.
- مجلة آي دي آر (IDR) البريطانية.
- مجلة فلايت انترناشونال (Flight International) البريطانية.
- مجلة سيانتيفيك أميركان (Scientific American) الاميركية.
- المجلات الكمبيوترية الأميركية والبريطانية بصورة عامة.

● كتب:

- أمن الكمبيوتر الصادر عن دار فكر.
- حرب الكمبيوتر في فلسطين.
- « عين واشنطن» لغابر يرنوكالفي وتيري بفستر.
- المنشورات المتعلقة بمنتجات الأمن الكمبيوتري بصورة عامة.
- الانظمة الحدية للمخابرات .
- حرب وحرب مضادة

(War & Anti- War, by Alvin & Heidi Toffler, Newyork, 1993)

- الكتب العسكرية العربية بصورة عامة.

حروب المستقبل

لقد بدأت الحروب ترتدي أشكالاً جديدة
تختلف اختلافاً جذرياً عما كانت عليه في الماضي
وذلك بفعل ظهور أسلحة الدمار الشامل وتزايد أهمية الاعلام
والتقنيات المعلوماتية، ويبحث هذا الكتاب في الجانب المعلوماتي
لأساليب الحروب المستقبلية.
كما أنه يلقي الأضواء على فئة جديدة من الأسلحة تعرف بالأسلحة
غير الفتاكة، وتتميز بأنها تقضي على قوة الاعداء من دون قتلهم.
ويقدم الكتاب أمثلة واقعية وتطبيقية حول التجارب العملية الأولى
للأسلحة الكمبيوترية وللأسلحة غير الفتاكة في الولايات المتحدة
وفي العالم العربي وفي يوغسلافيا، وهي أمثلة خطيرة ومهمة لا
يعرفها معظم الناس.

ويأتي «حروب المستقبل» متكاملاً مع كتاب «الأنظمة
الحديثة للمخابرات» ليعطي صورة واقعية
لنزاعات المستقبل

صدر للمؤلف:

- أمن الكمبيوتر
- اللوبي اليهودي في العالم
- حرب الكمبيوتر في فلسطين
- أسرار اللوبي اليهودي في العالم
- ملف اللوبي اليهودي في العالم
- الأنظمة الحديثة للمخابرات
- حروب المستقبل